Computer Viruses and Other Malicious Software

A THREAT TO THE INTERNET ECONOMY

OECD

Computer Viruses nd Other Malicious Software

THREAT TO THE INTERNET ECONOMY

GANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ECD is a unique forum where the governments of 30 democracies work address the economic, social and environmental challenges of globalisation s also at the forefront of efforts to understand and to help governments new developments and concerns, such as corporate governance, the economy and the challenges of an ageing population. The Organisation etting where governments can compare policy experiences, seek answers to roblems, identify good practice and work to co ordinate domestic and al policies.

ECD member countries are: Australia, Austria, Belgium, Canada, the ublic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, ly, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, land, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Kingdom and the United States. The Commission of the European es takes part in the work of the OECD.

Publishing disseminates widely the results of the Organisation's statistics nd research on economic, social and environmental issues, as well as the s, guidelines and standards agreed by its members.

OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*

Foreword

lressed primarily to policy makers, this book was developed over the
of 2007, by the OECD Working Party on Information Security and
(WPISP) in partnership with the Asia Pacific Economic Co-
n Telecommunication and Information Working Group (APEC
ecurity and Prosperity Steering Group (SPSG). The report was
fied by the Committee for Information, Computer and
nications Policy (ICCP) on 6 March 2008.

rafting the book, Audrey Plonk and Anne Carblanc from the OECD
iat have been assisted by Michel van Eeten of Delft University of
ogy and Johannes Bauer of Michigan State University, consultants
OECD, who have written Part II, and by a group of experts who
d feedback on Parts I and III. This group of experts included Mr.
Ingram and Ms. Kathryn Kerr (AusCERT), Mr. Colin Whittaker
S, UK Trade Association), Mr. Gilles André and Mr. Fabian Pouget
A France), Mr. Kevin Houle and Mr. Jeffrey J. Carpenter
CC), Mr. Erka Koivunen and Mr. Kauto Huopio (CERT-FI
), Dr. Pei-Wen Liu (Chinese Taipei), Mr. HyunCheol Jeong and Mr.
Cho (KrCERT/CC Korea), Mr. David Pollington, Mr. Jean-
phe Le Toquin and Mr. Uwe Manuel Rasmussen (Microsoft), Mr.
phe Birkeland (NORCERT Norway), Mr. Bill Woodcock (Packet
g House), and Mr. Jeremy Ward (Symantec Corporation). The
iat also benefited from the contribution of OECD and APEC
's, including Mr. Keith Besgrove and Ms. Sabeena Oberoi
ia), Mr. Shamsul Jafni Shafie (Malaysia), Mr. Jean-Jacques Sahel
Geoff Smith (United Kingdom), and Ms. Jordana Siegel and Mr.
Goldfarb (United States). The Dutch government made a special
ution to enable work on the economics of malware, which is
ly acknowledged.

Acknowledgements

ew study such as the one on the economics of malware (Part II) onsiderable debt along the way. First and foremost, we thank our wees, who gave generously of their time. They also provided comments on a draft version of this report and checked and d the use of their quotes where appropriate. Their input is greatly ated. To maintain confidentiality, none of those interviewed is named xt.

cial thanks go to our colleagues Mark de Bruijne, Wolter Lemstra n Groenewegen in Delft and Tithi Chattopadhyay, Yuehua Wu in nsing. They have provided invaluable contributions in the course of ject and we have greatly benefited from the exchanges of ideas with

also would like to thank Anne Carblanc, Audrey Plonk and Sam e at the OECD and Ronald van der Luit and Edgar de Lange at the nds Ministry of Economic Affairs for supporting this research and r engaging questions and comments. Selected findings from this re included in the OECD's report on *Malicious Software (Malware): ity Threat to the Internet Economy*, developed in collaboration with C Telecommunications Working Group.

have given presentations to conferences on our findings, including Telecommunications Policy Research Conference (Alexandria, VA, ber 28-30, 2007), the LAP/CNSA/MAAWG Workshop (Arlington, 9-11, 2007), the 2007 GOVCERT conference (Noordwijk, October 007). Some of the very best feedback has been from the presentation nterim findings at the meetings of the OECD WPISP and the ps with policy makers at the Dutch Ministry of Economic Affairs.

Table of Contents

Executive Summary

rred by the prevalence of always-on, high-speed connections, the has become a powerful tool for enhancing innovation and vity. The increasing dependence on the Internet and other nication networks, however, means the Internet has also become a and efficient way to distribute computer viruses and other types of us software.

ruses", "worms" and "zombies" might sound like science fiction, but in fact the reality presented by the spread of malware. The power eat of malware are that it can infiltrate, manipulate or damage al computers, as well as entire electronic information networks, the users' knowing anything is amiss.

of this has brought the electronic world to an important juncture slaught of malware attacks is increasing, both in frequency and cation, thus posing a serious threat to the Internet economy and to security. At the same time, current efforts to fight malware are not e task of addressing this growing global threat; malware response gation efforts are essentially fragmented, local and mainly reactive.

s report is a first step toward addressing the threat of malware in a hensive, global manner. As such, the report has three major aims: (1) m policy makers about malware – its growth, evolution and measures to combat it, (2) to present new research into the economic es driving cyber-security decisions; and (3) to make specific ons on how the international community can better work together to the problem.

need for a consistent approach to a global problem is not new, but presents particular challenges owing to the wide variety of actors on the problem: governments, businesses, end users and the

ight of the need for a holistic and comprehensive approach to
, a common point of departure is needed from which to build co-
n and collective action. This report calls for the creation of a global
Malware Partnership" involving governments, the private sector, the
l community and civil society.

malware

longer limited to the realm of computer hackers and tech researchers,
in the 2000s has become a serious business and a multi-million-
riminal industry. The major drivers can be summarised as follows:

ware is widely available. Virtually anyone can buy it online at a
cost, as well as from underground markets. And malware is user-
, meaning it provides attackers with the capability to launch
ed, sophisticated attacks beyond their skill level.

ware can infect all sorts of devices. Since it is nothing more than a
software, malware can infect not only personal computers but also
kbone of the Internet – the servers and routers that move data
de. While malware often propagates through the Internet, it is
nt to note it can also be introduced into computer systems not
ed to the Internet.

ware is profitable. Together with other cyber tools and techniques,
is a low-cost, reusable way to carry out highly lucrative forms of
me. Two prime examples are the capture of credit card and bank
data via "spyware" and the launch of "denial-of-service" attacks
extort money or concessions.

ware can harm critical information infrastructures, cause major
l losses and, perhaps worst of all, undermine trust and confidence in
rnet economy. Therefore, malware is increasingly a shared concern
nternet market participants: governments, businesses and individuals
OECD countries and Asia Pacific Economic Co-operation (APEC)
ies.

ernments, for one, are increasingly dependent on the Internet for
g services, making them and their citizens vulnerable to malware. In
to the complex and expensive task of securing their own systems,

mmerce companies to software vendors – have had to increase -related investments in order to expand their online business.

key Internet market participants interviewed for this book (please II) were devoting an estimated 6% to 10% of their technology to protect against malware. Combined with indirect costs (such as watchdog organisations, public education campaigns and law nent efforts) the total costs of malware for key Internet market ants may well be above 10% of technology spending.

trends

explained in Part I, the deployment of malware is becoming ever- ophisticated and targeted, presenting a great challenge to those ng to measure and combat the problem. Key findings include:

Self-sustaining cyber attacks increasingly depend on "botnets", or groups of malware-infected computers (also called "zombies") that can be used to remotely carry out attacks against other computer systems.

Many malware attacks are smaller and deliberately limited in scope, in an attempt to stay "below the radar" of the security and law enforcement communities.

Spam has evolved from a nuisance, to a vehicle for fraud, to a vector for distributing malware.

The overall malware problem is difficult to quantify: no single entity has a global understanding of the scope, trends, development and consequences of malware.

Data on malware are not consistent, and terminology for cataloguing and measuring the occurrence of malware is not harmonised.

The effectiveness of current approaches in combating malware is constantly challenged by both ongoing technological changes and faster exploitation of software vulnerabilities.

economic incentives

a great extent, cyber security is affected by the behaviour of the key market participants: Internet Service Providers, e-commerce ies, domain name registrars, software vendors, and end users. Part II

at trade-offs are associated with these responses, and how the ation is affected by the security actions of other market participants. ey findings were:

How key market participants address malware is greatly influenced by the specific incentives they face: greater online traffic vs. higher security costs, for example. Some of these incentives work to enhance online security while others work to reduce it.

In many instances, market participants make decisions that pass on the costs of malware to others in the network (thus "externalizing" them), such as when end users opt not to protect their computers against viruses.

Owing to existing feedback loops, which should be strengthened and expanded, the extent of passed-on costs and benefits is probably smaller than had been previously assumed. On the other hand, many of these passed-on costs remain unaddressed.

proach

le this work details many of the problems presented by malware, it a first step towards a solution. To prevent malware from becoming a threat to the Internet economy and to national security, a global hip against malware is needed.

vide range of communities and actors – from policy makers to Service Providers to end users – all play a role in combating . But there is still limited knowledge, understanding, organisation neation of the roles and responsibilities of each of these actors.

refore, a global "Anti-Malware Partnership" should involve not only ients, but also the private sector, the technical community and civil Such an inclusive, co-ordinated effort would be more likely to co-ordinated policy guidance to fight malware on all fronts – from onal to technical to legal and economic.

type of international co-operation should be supported and d by accurate measurement of the problem and analysis of the ng economics at play. Also, the limitations of current actions against should be addressed, and the question of how to strengthen anti- incentives for market participants should be further explored.

rovements can be made in many areas, and international co-

Background

Organisation for Economic Co-operation and Development
) Working Party on Information Security and Privacy (WPISP) and
ıia Pacific Economic Co-operation Telecommunication and
tion Working Group (APEC TEL) Security and Prosperity Steering
SPSG) have both experience and expertise in the development of
uidance for the security of information systems and networks

2002, the OECD adopted the *Guidelines for the Security of*
tion Systems and Networks ("the *Security Guidelines*") which
a clear framework of principles at the policy and operational levels
consistent domestic approaches to addressing information security
a globally interconnected society. More broadly, the *Security*
nes reflect a shared ambition to develop a culture of security across
so that security becomes an integral part of the daily routine of
uals, businesses and governments in their use of Information and
mication Technologies (ICTs) and in conducting online activities [1]. In
d 2005, the OECD monitored efforts by governments to implement
policy frameworks consistent with the *Security Guidelines*,
g measures to combat cybercrime, develop Computer Security
Response Teams (CSIRTs), raise awareness, and foster education
as other topics (OECD, 2005a). In 2006 and 2007, the OECD
on the development of policies to protect critical information
ıctures (OECD, 2007c and 2008).

ewise, in 2002, APEC issued the APEC Cybersecurity Strategy
g six areas for co-operation among member economies including
evelopments, information sharing and co-operation, security and
l guidelines, public awareness, and training and education. To
ıent the APEC Cybersecurity Strategy, in 2005 the APEC TEL
the Strategy to Ensure a Trusted, Secure, and Sustainable Online

CD and APEC objectives

2005, the APEC and OECD co-organised a workshop to share tion on evolving information security risks and to explore areas for co-operation between the organisations to better tackle the onal dimension of information security risks. In 2006, both ations agreed that the need to encourage a safer and more secure environment was more pressing than ever due to the continued of economic and social activities conducted over the Internet and the d severity and sophistication of online malicious activity. ently, they decided to organise a workshop[2] and develop an al report to examine the issues of malicious software, commonly as "malware", with a view to:

- Informing national policy makers on the impacts of malware
- Cataloguing trends in malware growth and evolution
- Examining the economics of malware and the business models behind malicious activity involving malware
- Evaluating existing technical and non-technical countermeasures to combat malware and identify gaps; and,
- Outlining key areas for action and future work.

pared by the OECD Secretariat in close collaboration with volunteer ent experts from OECD and APEC as well as the private sector, ort does not discuss every aspect of malware, all types of malware, opagation vectors. Rather, it focuses on issues of significant concern as which may pose problems in the future. Similarly, the report does mine all possible strategies associated with preventing, detecting and ng to malware but rather focuses on elements of relevance to OECD countries, APEC economies, and other governments and ations more broadly. Finally, the report refers to forms of me, such as spam and phishing[3] that may not *directly* involve the alware but nevertheless demonstrate how malware can also be used y to facilitate cybercrime.

Notes

ıe United Nations, the Council of the European Union, the Asia Pacific onomic Co operation (APEC) and the Asia Europe Meeting (ASEM) l recognised and used the Guidelines in their work.

formation on the joint APEC-OECD Malware Workshop is available at *ww oecd org/document/34/0,3343,en_2649_34255_38293474_1_1_1_1, html*

ıishing refers to a social engineering attack, where an attacker ampulates a user to disclose their online account access credentials or her personal information (typically) to a website in the control of an tacker. According to this definition phishing may not *directly* involve alware. However, when the term is used to, for example, also refer to rtain types of Trojan attacks, malware is implicated.

Part I. The Scope of Malware

of this book defines the various forms of malicious software re) and their impact, growth and evolution. Specifically, Chapter 1 the major types of malware, Chapter 2 focuses on the types of attacks possible and their perpetrators, and Chapter 3 explains the malware takes on the information and communications industry, as why malware is a growing and major concern for governments, es and citizens of OECD countries and APEC economies

Chapter 1. An Overview of Malware

ware?

ware is a general term for a piece of software inserted into an tion system to cause harm to that system or other systems, or to them for use other than that intended by their owners [1]

ware can gain remote access to an information system, record and ta from that system to a third party without the user's permission or lge, conceal that the information system has been compromised, security measures, damage the information system, or otherwise e data and system integrity

erent types of malware are commonly described as viruses, worms, horses, backdoors, keystroke loggers, rootkits or spyware. These orrespond to the functionality and behaviour of the malware (*e.g.* a self propagating, a worm is self replicating).[2] Experts usually group into two categories: family and variant. "Family" refers to the or original piece of malware, "variant" refers to a different version iginal malicious code, or family, with minor changes.[3]

characteristics of malware

ough not the only means by which information systems can be mised, malware provides attackers convenience, ease of use, and ion necessary to conduct attacks on a previously inconceivable

ware is multi-functional and modular: there are many kinds of that can be used together or separately to achieve a malicious goal. New features and additional capabilities are easily added to to alter and "improve" its functionality and impact (Danchev,

Box 1.1 Malware: a brief history

ses and worms date back to the early days of computers when most were created for fun and worms were created to perform maintenance on er systems. Malicious viruses did not surface until the 1980s when the rsonal computer (PC) virus, Brain (1986), appeared and propagated when r "booted up" his/her computer from a floppy disc. Two years later, in he Morris worm received significant media attention and affected over 6 mputers. Although other types of malicious software appeared in the mid he landscape of the late 80s and early 90s predominantly consisted of . Until about 1999, most people related viruses to the example of a r hacking into the Pentagon's systems as seen in the 1983 movie nes.

e mid to late 1990s, the landscape began to change with the growth of the and personal computer use, the rise of networking, and the adoption of ic mail systems. The so-called "big impact worms" began to reach the n novel ways. The increased use of e-mail brought high-profile mass-worms such as Melissa (1999), "I Love You" (2000), Anna Kournikova SoBig (2003) and Mydoom (2004) that made the headlines and entered lic consciousness. These types of worms doubled their number of victims ne-to-two hours, rapidly reaching peak activity within 12-to-18 hours of eleased. This marked the parallel rise in organised, sometimes co-ed attacks. The explosive growth of online financial transactions resulted ased security incidents and in the appearance of new types of malicious e and attacks. Today, mass worms and virus outbreaks are becoming ever while stealthy malware such as Trojans and backdoors are on the rise. ttacks are smaller to stay "below the radar" of the security and law ment communities. The goals of the attackers tend to be focused on l gain. These new trends help explain why malware is now a global multi-dollar criminal industry.

lware is available and user-friendly: malware is available online at al cost thus making it possible for almost anyone to acquire. There is robust underground market for its sale and purchase. Furthermore, e is user-friendly and provides attackers with a capability to launch cated attacks beyond their skill level.

ware is persistent and efficient: malware is increasingly difficult to nd remove and is effective at defeating built-in information security

lware can affect a range of devices because malware is nothing an a piece of software, it can affect a range of devices, from personal such as personal computers (PCs) or Personal Digital Assistants to servers[6] across different types of networks All these devices, g the routers that allow traffic to move across the Internet to other nts, are potentially vulnerable to malware attacks

lware is part of a broader cyber attack system malware is being th as a primary form of cyber attack and to support other forms of us activity and cybercrime such as spam and phishing Conversely, d phishing can be used to further distribute malware

lware is profitable malware is no longer just a fun game for script or a field of study for researchers Today, it is a serious business rce of revenue for malicious actors and criminals all over the world e, together with other cyber tools and techniques, provides a low isable method of conducting highly lucrative forms of cybercrime

lware work?

ware is able to compromise information systems due to a ation of factors that include insecure operating system design and software vulnerabilities Malware works by running or installing an information system manually or automatically[8] Software may vulnerabilities, or "holes" in its fabric caused by faulty coding e may also be improperly configured, have functionality turned off, in a manner not compatible with suggested uses or improperly ed with other software. All of these are potential vulnerabilities and for attack Once these vulnerabilities are discovered, malware can be ed to exploit them for malicious purposes before the security nity has developed a "fix", known as a patch Malware can also mise information systems due to non-technological factors such as r practices and inadequate security policies and procedures

ny types of malware such as viruses or Trojans require some level of eraction to initiate the infection process such as clicking on a web n e-mail, opening an executable file attached to an e-mail or visiting e where malware is hosted Once security has been breached by the nfection, some forms of malware automatically install additional ality such as spyware (e.g. keylogger) backdoor rootkit or any

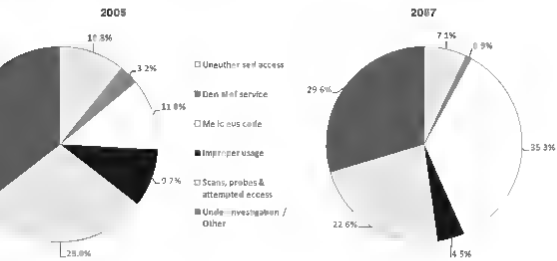
ey have received a notice from their bank, or a virus warning from em administrator, when they have actually received a mass-mailing Other examples include e-mail messages claiming to be an e-card unspecified friend to persuade users to open the attached "card" and ad the malware

ware can also be downloaded from web pages unintentionally by A recent study by Google that examined several billion URLs and d an in-depth analysis of 4 5 million found that, of that sample, 700 med malicious and that 450 000 were capable of launching malicious ads (Google, Inc. p 2). Another report found that only about one in bsites analysed were malicious by design. This has led to the on that about 80% of all web-based malware is being hosted on t but compromised websites, unbeknownst to their owners (Sophos, 4)

ifferent report found that 53 9% of all malicious websites observed ed in China (Sophos, 2007, p 6) The United States ranks second in e study with 27 2% of malicious websites observed located in there more, the data provided below demonstrates that by mid-2007 on web pages accounted for 58 2% of the incident reports received Jnited States Computer Emergency Readiness Team (US-CERT)

1 US-CERT Incident reporting trends for January 2006 - August 2007

Distribution of cybersecurity incidents and events across the six major categories

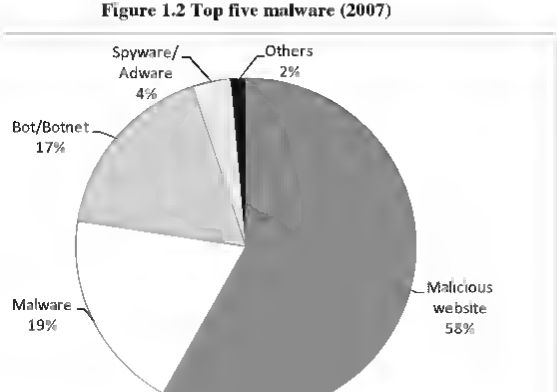


IST (2008)

umber of incidents involving malware (malicious code) has ntly increased from 2006 to 2007.

re 1.2 below depicts the top five malware sub-categories being to US-CERT. The category labelled as "Malware" includes worms and viruses. The graph shows "Malicious websites" as the mmonly reported sub-category.

Figure 1.2 Top five malware (2007)



US CERT

United States Computer Emergency Readiness Team ERT)?

artnership between the Department of Homeland Security (DHS) public and private sectors. Established in 2003 to protect America's infrastructure, US-CERT co-ordinates defense against and es to cyber attacks across the nation. The organisation interacts with agencies, state and local governments, industry professionals, and o improve information sharing and incident response co-ordination

e propagation vectors

ware propagation vectors refer to the electronic methods by which
is transmitted to the information systems, platforms or devices it
infect Email and instant messaging applications are some of the
ommon vectors used for spreading malware through social
ring techniques Any medium that enables software to be distributed
d, however, can be a vector for malware Examples of malware
tion or distribution vectors include the World Wide Web (WWW),
ble media (such as USB storage keys), network-shared file systems,
sharing networks, Internet relay chat (IRC), Bluetooth or wireless
ea networks (WLAN) [11]

etooth is one prominent vector for malware propagation on mobile
Bluetooth is a wireless personal area network (PAN) that allows
such as mobile phones, printers, digital cameras, video game
, laptops and PCs to connect through unlicensed radio frequency
ort distances Bluetooth can be compromised by techniques such as
ing and bluesnarfing[12] and is most vulnerable when a user's
on is set to "discoverable" which allows it to be found by other
luetooth devices [13]

Box 1.2 Examples of malware propagation vectors

Malware can be "mass mailed" by sending out a large number of e-mail with malware attached or embedded There are numerous examples of l malware propagated through mass-mailers largely due to the ability of actors to use social engineering to spread malware rapidly across the globe

Attackers are increasingly using websites to distribute malware to potential This relies on spam e-mail to direct users to a website where the attacker has malware capable of compromising a computer by simply allowing a browser n to the website If the website is a legitimate and popular site, users will go their own accord allowing their computers to potentially become ompromised without the need for spam e-mail to direct them there There nethods of infection via the web: compromise existing web site to host or set up a dedicated site to host malware on a domain specially registered irpose

messengers Malware can propagate via instant messaging services on the y sending copies of itself through the file transfer feature common to most essenger programmes Instant messages could also contain web links that user to another site hosting downloadable malware Once a user clicks on a layed in an instant messenger dialog box, a copy of the malware is

x 1.2 Examples of malware propagation vectors (continued)

ork-shared file systems A network share is a remotely accessible digital rage facility on a computer network A network share can become a hability for all network users when access to the shared files is gained by us actors or malware, and the network file sharing facility included within rating system of a user's computer has been otherwise compromised

programmes Some malware propagates itself by copying itself into it assumes to be shared (such as those with share in its folder name), or for it activates sharing, and uses an inconspicuous or invisible file name y posing as a legitimate software, or as an archived image)

net Relay Chat (IRC) IRC is a form of Internet chat specifically designed oup communications in many topical "channels," all of which are ously and anonymously available from any location on the Internet Many nasters' (as the malefactors who operate networks of malware- l/compromised machines are often called, see the chapter "The Malware - Botnets") use IRC as the central command and control (C&C) nications channel for co-ordinating and directing the actions of the bot l/compromised information systems in their 'botnet"

tooth Bluetooth is a wireless networking protocol that allows devices like phones, printers, digital cameras, video game consoles, laptops and PCs to at very short distances, using unlicensed radio spectrum Because the mechanisms implemented in Bluetooth devices tend to be trivially ed, such devices are vulnerable to malware through attack techniques nave been called "bluejacking" or "bluesnarfing." A bluetooth device is ulnerable to this type of attack when a user's connection is set to erable" which allows it to be found by other nearby bluetooth devices

less local area network (WLAN) Wireless LAN or WLAN is a wireless ea network, which is the linking of two or more computers without using WLAN utilises spread spectrum or OFDM (802.11a) modulation ogy based on radio waves to enable communication between devices in a area, also known as the basic service set This gives users the mobility to round within a broad coverage area and still be connected to the network

mobile devices

re is some debate around the current seriousness of threats to mobile such as cell phones, PDAs, and smartphones.[14] For example, some seem to indicate that threats to mobile devices are still limited These include the following

mobile devices are restricted by bandwidth because there is a limited amount of spectrum allocated for their use,

the very small user interface is still an impediment to conducting Internet banking and other value transactions – until mobile devices become a popular means to conduct such transactions there are fewer incentives for attackers to develop malware for the mobile telephone platform[16],

the cost associated with using general packet radio service (GPRS) to connect to Internet Protocol (IP) data networks may also make the mobile device less popular compared to Internet-connected PC which use technologies such as asymmetric digital subscriber line (ADSL), cable or broadband wireless

vever, there is also recognition that such threats, while emerging, are al. Some data show that although still relatively small in comparison mount of PC malware, mobile malware, which first appeared in creased from only a few instances to over 300 in total in a two-year Hypponen, 2006).

her, concerns about security increase as mobile devices become evalent and are used to access more critical or 'valuable' services [17] mple, the use of smartphones is on the rise with projections as high million in use by 2009 (Hypponen, 2006). In 2006, Apple announced number of video iPods had been shipped to customers with the nE virus.[18] Many experts are concerned that mobile malware will come far more dangerous to the mobile devices themselves, the networks over which those devices communicate and the corporate s, servers and/or personal computers with which those devices e information. Undetected malware on a smartphone could get ed to a corporate network and used to perform further malicious s (iGillottResearch Inc, 2006).

re Internet: botnets

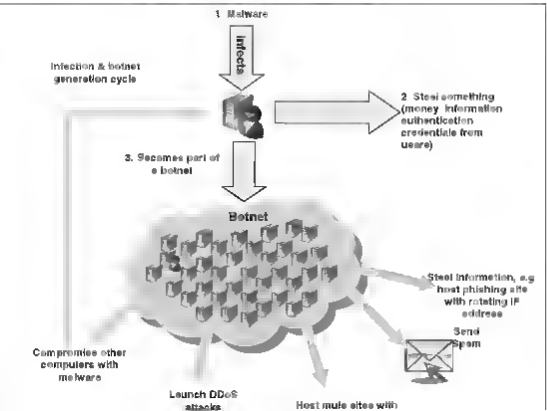
s a botnet?

ow prevalent form of malware, botnets are key tools attackers use to a variety of malicious activity and cybercrime. A botnet is a group vare infected computers also called "zombies" or bots that can be

ommonly referred to as "bot herders" or "bot masters" that can
he botnet remotely The bots are then programmed and instructed by
herder to perform a variety of cyber attacks, including attacks
g the further distribution and installation of malware on other
tion systems Malware, when used in conjunction with botnets,
attackers to create a self-sustaining renewable supply of Internet-
ed computing resources to facilitate their crimes (see Figure 3)
f the malware discussed earlier in this report is distributed using
There is thus a cyclical relationship malware is used to create
and botnets are used to further distribute spam and malware

ure 1.3 demonstrates the relationship between malware and the
ifecycle When malware infects an information system, two things
ppen something can be stolen (*e.g.* information, money,
cation credentials etc) and the infected information system can
part of a botnet When an infected information system becomes part
net it is then used to scan for vulnerabilities in other information
connected to the Internet, thus creating a cycle that rapidly infects
ble information systems

Figure 1.3 The botnet lifecycle



otnets used for?

nets are mostly used for the following purposes.

Locate and infect other information systems with bot programmes (and other malware). This functionality in particular allows attackers to maintain and build their supply of new bots to enable them to undertake the functions below, *inter alia*

Conduct distributed denial of service attacks (DDoS).

As a service that can be bought, sold or rented out

Rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent web sites, in which for example host phishing and/or malware sites

Send spam which in turn can distribute more malware

Steal sensitive information from each compromised computer that belongs to the botnet

Hosting the malicious phishing site itself, often in conjunction with other members of the botnet to provide redundancy

Many botnet clients allow the attacker to run any additional code of their choosing, making the botnet client very flexible to adding new attacks.

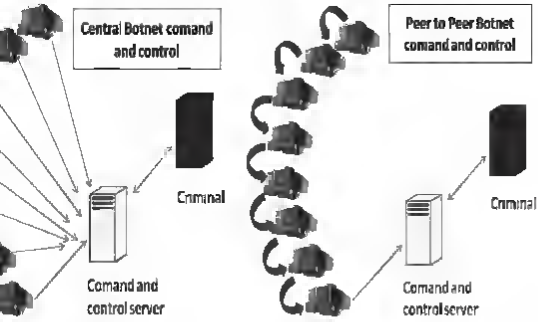
mmand and Control (C&C) models

ically, bots communicate with the bot master through an Internet hat (IRC) command and control (C&C) server which provides the ons directing the operation of the botnet. The C&C server usually is lf a compromised computer running various network services. After ter system is infected and compromised by a bot program, the bot ally connects back to the C&C server, checking for instructions. h there are various C&C models, the most popular has traditionally centralised model (see Figure 1.4) where all bots report to a single to wait for commands. The centralised model is popular among bot because it offers software tools that make it easy to operate nore, the centralised model results in few communication delays the bot master and the bots (Trend Micro, 2005). Increasingly

nications to or from their network as it is hidden among the vast of normal web traffic.

alternative innovative C&C model designed to make it more difficult rity practitioners to stop botnet hosted attacks is the increasing use eer to peer (P2P) model (see Figure 1 4) (Govcert nl, 2007) The eer model lacks a central hierarchy of communication which makes et more resilient to dismantling (Trend Micro, 2005). it is therefore ly difficult to stop attacks launched from botnets that communicate 2P as there is no single point of failure

Figure 1.4 Command and control for botnets



ddition to the models above, botnets are increasingly using what is as "fast flux" networks to evade detection. Fast flux networks are s of compromised computer systems with public DNS records that constantly thus making it more difficult to track and shut down us activity (The Honeynet Project, 2007). Furthermore, this model as the traditional centralised C&C server and uses proxies to hide the controlling the fast flux network.

es

rs are connected to the Internet, whether they have been "cleaned", her the attacker is using his botnet to locate and compromise more tion systems to add to the botnet. Furthermore, there are incentives herders to use smaller botnets and launch smaller, more targeted, to avoid detection. For example, large botnets sending spam or ng DDoS attacks generate a high volume of network traffic that is detectable by ISPs and network administrators, whereas smaller hat use less bandwidth may go undetected.

nets have become a contracted commodity. Malicious actors can hire bot master to carry out an attack. One report averaged the weekly te for a botnet at USD 50-60 per 1 000-2 000 bots, or around 33 per compromised computer (MessageLabs, 2006). This is dnarily cheap compared to the cost of the computer to the legitimate terms of hardware, software and bandwidth.

Box 1.3 The Dutch botnet case

ctober 2005 the Dutch National Police arrested three men – members of a of cyber criminals – suspected of large scale "hacking". The men ed several botnets that were thought to have consisted of over 1.5 million computers. The botnets played a key role in numerous cyber crimes ng phishing, identity theft, online fraud, and online extortion. In due it became clear that botnets played a central role in the activities of the riminals by serving as the basic infrastructure that allowed for the ful attacks.

ne 2005 a report was made to the CERT community in the Netherlands important Netherlands based computer centre had been hacked. The community in turn reported the incident to the High Tech Crime Unit ly the Dutch National High Tech Crime Center) of the Dutch National

d on information combining IP addresses and the name of the suspect broadband Internet connection in use at his home address, the prosecutor y requested the interception of Internet traffic in order to collect more e. To determine the size of the botnet and the illegal activities of the , all IRC protocol traffic in the intercepted data was analysed. It was clear s botnet was very large and used multiple IRC channels on multiple IRC . In this specific investigation, the team realised that the criminals ed at least two large botnets used for their cyber crimes and that even after nding the criminals, the possibility existed that the botnets would still be

prevalence of botnets has been increasing. Although estimates of
ıber of botnets can vary widely, most experts agree it is a large
For example, in 2006, the Chinese National Computer Network
ncy Response Technical Team Coordination Center (CNCERT/CC)
that 12 million IP addresses in China were controlled by botnets
07). They also found more than 500 botnets and more than 16 000
ommand and control servers outside China.

broadband

increased threat of botnets can partially be explained by the
d use of broadband connections to access the Internet. Further
re needed from users, as well as providers, to protect their security
vacy in the online environment. By 2004, broadband Internet
ions were already widespread in OECD countries. For example, in
86% of households and 92% of businesses had a broadband
ion via a computer or mobile phone in 2004 (OECD, 2005). In the
g two years, those numbers have continued to increase. At the end
, there were around 265 million active subscribers to fixed Internet
ions in OECD countries. Of these, 60% were using broadband
and broadband subscriptions have increased by more than 60% a
r the last five years. By mid-2006, there were more than 178 million
nd subscribers in the OECD area. European countries have
d to advance, with Denmark, the Netherlands and Iceland
ng Korea and Canada in terms of broadband penetration rates over
year (OECD, 2007).

broadband transition to faster upload bandwidth via fibre could
e botnet problem much more severe. The potency of one infected
r on a fibre connection could be equivalent to 31 infected computers
and 44 computers on cable networks.[21] This will be one of the key
f concern for policy makers dealing with telecommunication
s and security in the near future.

otnets

re is a correlation between botnets and spam due to changes in

(Sophos, 2006a) For example, the second most common malicious mily reported from January - June 2006, Bomka, was a Trojan adable from a link provided in a spam e-mail that used social ring techniques to persuade the user that the link was the site of a lip (Symantec, 2006). The problem of spam and malware is also and self-sustaining. Information systems compromised by malware l to distribute spam and a proportion of the spam that is distributed is d to distribute malware to new victims whose information systems ised to undertake further online malicious activity.

important to note that not all spam contains malware, and it is often to determine how much spam *directly* contains malware. Manual conducted by The Information and Communication Security ogy Center (ICST) in Chinese Taipei over the course of two years suspect e-mails found that of those 417 analysed, 287 (68%) d malware attachments (Liu, 2007, p. 3).[22] Other data shows that in nly 1.5%, or 1 in every 67.9 e-mails analysed, contained a virus or and according to the same report, in 2005 the annual average was r 1 in every 36.1 (MessageLabs, 2006). It is likely that the disparate f these findings can be explained by a lack of comparable techniques mine when spam contains malware.

ently, the Messaging and Anti-Abuse Working Group (MAAWG) that the percentage of email identified as "abusive"[23] has been ng between 75% and 80% (Messaging Anti-Abuse Working Group, They attribute the fluctuation to service providers dealing with new introduced by abusers to escape service providers' detection s, including filters. Nonetheless, it is widely accepted that the vast of spam is sent from botnets. The effectiveness and wide lity of compromised information systems with high speed broadband ions means that spam levels are at their highest levels ever despite atives to reduce and prevent spam being distributed.

ough civil enforcement against spam, such as the case described s important, most instances of malware are inherently criminal, and law enforcement agencies are best suited to expertly shut down minal operations.

Box 1.4 FTC v. Dugger

ne recent case, the US Federal Trade Commission (FTC) sought to stop the ing use of botnets to send spam (FTC v Dugger) The FTC alleged that endants relayed sexually explicit commercial e mails through other home computers without their knowledge or consent They further that the defendant's conduct violated the CAN SPAM Act Under the final the defendants were barred from violating the CAN SPAM Act and to turn over USD8 000 in profits made through use of the botnet The nts were also required to obtain the authorisation of a computer's owner using it to send commercial e-mail and to inform the owner how the er will be used

blacklists in combating botnets

klisting is a loosely used term typically referring to the practice of -called DNS Blacklists (DNSBL) to filter incoming Internet traffic rvers may be configured to refuse mail coming from IP addresses, IP or whole networks listed on a specific DNSBL There is a wide of blacklists that may be used in different combinations

t of the lists are free and run by volunteers, though their operations funded through external sources Each DNSBL has its own criteria ding an IP address in the list and its own procedure for getting an off the list Spamhaus, an international non-profit organisation through sponsors and donations, maintains several well-known ts – though they prefer the term block lists – which they claim are protect over 600 million user inboxes One of their lists contains the s of "spam-sources, including spammers, spam gangs, spam ns and spam support services"; another list focuses on botnets which n proxies It should be noted at this point that blacklisting, while lly powerful, has drawn its own criticisms – regarding, among other igilantism of blacklist operators, listing false positives, the collateral that may come with blacklisting certain IP addresses or ranges, and ncial motives of some list operators Furthermore, blacklists have gal challenges from spammers, who on occasion were successful in g court verdicts against being blacklisted According to interviewees

sting and ISPs[24]

klisting does provide an incentive to invest in security because it impacts an ISP's business model. For example, one medium-sized orted a security incident where 419 spammers[25] set up over 1 000 e- ounts within their domain and then started pumping out spam. That ISP's outbound mail servers blacklisted, which resulted in a high of calls to their customer centre by customers who noticed their e- as no longer being delivered. That number doesn't include the g abuse notifications, of which there were purportedly "even more." ier example, a security officer at a large ISP explained that being ted led to a much more proactive approach to remove bots from their , including the purchase of equipment that automates the process of ing infected machines on the network (Eeten and Bauer, 2008). In 07, this particular ISP identified around 50 customers per day and, if omer did not resolve the problem, the connection was suspended.

re are various levels of blacklisting used to incite a response from an the lower end, there is blacklisting of individual IP addresses, *i.e.*, an ual customer. This has "exactly zero impact on the ISP," said a expert. Only when the number of listed IP addresses reaches a hreshold might the problem get an ISP's attention. According to the ISPs mostly ignore listed individual IP addresses, because of the y high costs of dealing with them (*e.g.* through customer support). nore, particular IP addresses get taken off the blacklist as spammers kers move on to other infected machines.

re powerful incentives are the blacklisting of whole IP ranges and of d mail servers. These typically do get the ISPs' attention and lead to l action on their end, though the effectiveness varies with the degree ance applied by the ISP. The most extreme form is blacklisting an etwork (*i.e.*, all IP addresses of an ISP). This is only used against ultimate ISPs who do not act against spam, and against known spam

sting and Domain Name Registrars

istrars offering hosting and e-mail services are subject to ting along the same lines as the ISPs. Blacklist operators also watch s and their responsiveness to abuse complaints. In extreme cases,

ıc at did not comply with these requests, citing legal constraints. The argued that it could not legally remove the sites, unless Spamhaus d clear proof that the domain names had been registered using false tion (Sokolov, 2007). The conflict escalated when Spamhaus added ound mail server of Nic.at to one of its blacklists – listing them as upport" – so that the registrar's e-mail was no longer accepted by titude of servers using this popular blacklist. About ten days later us changed the listing of Nic.at to a symbolic listing – no longer blocking the IP addresses, but keeping them listed as "spam ". Several of the offending domains had been removed, but Nic.at hat it had complied with Spamhaus' request and asserts that the providers took action (ORF, 2007, Spamhaus, 2007).

Notes

ne 1992 OECD *Guidelines for the Security of Information Systems and etworks* defined an information system as computers, communication cilities, computer and communication networks and data and formation that may be stored, processed, retrieved or transmitted by em, including programmes, specification and procedures for their peration, use and maintenance.

e the Glossary of Malware Terms at the end of this book.

or example, W32.Sober@mm (also known as Sober) was the primary urce code of the "Sober" family. Sober.X is a variant of Sober. (See ymantec, 2006, p.67).

ost refers to a computer at a specific location on a network.

e Chapter 2 for a discussion of digital certificates.

rvers are generally more powerful computers which provide services to nd accept connections from) many clients however home PCs and rporate workstations can also act as servers, particularly when they come compromised. Common types of servers include web, e-mail and tabase servers.

ript Kiddie refers to an inexperienced malicious actor who uses

alware may also exploit vulnerabilities in hardware, however, this is re compared to the number of software vulnerabilities which are ailable at any given time to exploit

e the Glossary of Malware Terms at the end of this book

cial engineering refers to techniques designed to manipulate users into oviding information or taking an action which leads to the subsequent each in information systems security

e Box 1 2 for additional detail of propagation vectors

uejacking consists in sending unsolicited messages to Bluetooth nnected devices Bluesnarfing enables unauthorised access to formation from a wireless device through a Bluetooth connection

hile Bluetooth can have a range of 100 metres for laptops with powerful nsmitters, it has a more limited range for mobile phones, usually ound 10 metres

Smartphone is a cellular phone coupled with personal computer like nctionality

personal area network (PAN) is a computer network used for mmunication among computer devices (including telephones and rsonal digital assistants) close to one person The devices may or may ot belong to the person in question The reach of a PAN is typically a w meters PANs can be used for communication among the personal vices themselves, or for connecting to a higher level network and the ternet

hese transactions are possible as is demonstrated by the Japanese arket See BBC (2007)b)

or example, some financial institutions that wish to implement nsaction signing and avoid providing customers with a separate smart rd reader, may in future provide support for transaction signing through e use of a customer's own mobile telephone PDA In this way, the obile PDA also is likely to be targeted to subvert the transaction signing ocess As discussed in the glossary, transaction signing is only effective the keyed hash for the transaction is calculated on a device that can be usted

ote that the virus was transmitted to the device through a Windows mputer on the production line See *tp://www.apple.com/support/windowsvirus/*

ecutes automated tasks It is most widely used in the context of Internet
lay Chat (IRC) where users can create and use bot scripts for online
ming, co–ordinating file transfers, and automating channel admin
mmand (EggDrop is one of the oldest of such benign IRC bots) The
ct that botnets often rely on IRC bots for command and control by
otmasters might explain why the term "bot" is so popular in the literature
d discussions related to malware

is is the same protocol that enables both encrypted (https) and
encrypted (http) web based communications to occur Blocking this
ffic would prevent web access to a network

ne infected computer on a fibre connection with 100 Mbit/s of upload
pacity could theoretically cause as much damage as 390 infected
mputers with upload speeds of 256 kbit/s The average advertised
load speeds for broadband in the OECD in October 2006 was 1 Mbit/s
r DSL, 0 7 Mbit/s for cable and 31 Mbit/s for FTTx

ote that this data is based on self-selected spam that fits a certain
tegory or type and therefore is representative of a smaller sample set
rthermore, this data does not include the mass mailing worms/viruses

AAWG uses the term "abusive" because definition of spam can vary
eatly from country to country

is text has been extracted from the original report See Eeten, M J van
d J M Bauer (2008), pp 33-34

is is an advance-fee fraud in which the target is persuaded to advance
latively small sums of money in the hope of realizing a much larger
in Among the variations on this type of scam are the Nigerian Letter
r 419 fraud) The number "419" refers to the article of the Nigerian
riminal Code dealing with fraud

pter 2. Malware Attacks: Why, When and How?

lware attacks

numerous types of malware can be used separately or in ation to subvert the confidentiality, integrity and availability of tion systems and networks Likewise, a range of different attacks can ducted to reach different goals, such as denying access to critical tion systems, conducting espionage, extorting money (*e.g.* ransom), ing information (*e.g.* ID theft). Malware can also be used to mise authenticity and non-repudiation, or conduct attacks on the Name System (DNS).[1]

g access

ying access to digital data, network resources, bandwidth, or other services (denial of service – DoS) is a common goal of attacks alware. Popular targets include companies that conduct business nd risk losing significant revenue for every minute their website or is unavailable, and governments who rely on websites to provide l services to their citizens. These attacks are usually used for e (for example, to hurt a competitor or an organisation against whom cker holds a grudge or grievance), extortion, or for politically and cally motivated purposes (Messmer and Pappalardo, 2005).

uted Denial of Service (DDoS) attacks

most well known and perhaps most common method to deny access buted denial of service attacks (DDoS). DDoS attacks seek to render anisation's website or other network services inaccessible by elming them with an unusually large volume of traffic.[2] Malware y contributes to DDoS attacks by creating a renewable supply of

the service unavailable to most or all of its legitimate users, or at grading performance for everyone

ple DDoS attacks use a distributed network of bots (called a botnet) k a particular target The more complex DDoS attacks use multiple to simultaneously attack the target In traditional DDoS attacks, are used to send massive amounts of queries and overwhelm a However, low and slow attacks, a recent trend noted by some experts, occur over a longer period of time and use a small amount width from thousands, if not millions, of compromised computers he attacker co-ordinates the attack so that not all the bots will attack et at the same time, but rather on a rotating basis The victim and the Service Provider may not notice that their network traffic has d but over time, it becomes a drain on their infrastructure and other es

Box 2.1 The Estonian case

lay 2007, a series of cyber attacks were launched against Estonian nent and commercial websites Some attacks involved defacing websites, acing the pages with Russian propaganda or bogus information Up to six re rendered inaccessible at various points, including those of the foreign ice ministries Most of the attacks were launched using botnets comprised thousands of ordinary computers

nia's computer emergency response team (EE-CERT) acted swiftly and, in ation with partners from the international community, was able to weather rious attack with little damage The attack was primarily defended through – blocking connections from outside Estonia For example, Estonia's argest bank, SEB Eesti Uhispank, blocked access from abroad to its online service while remaining open to local users One major contributor to the of their services domestically during the attack was the fact that Estonia domestic Internet exchange points (IXPs)[4]

weeks after the attacks ended, one researcher identified at least 128 attacks on nine different websites in Estonia Of these 128 attacks, 35 portedly against the website of the Estonian Police, another 35 were ly against the website of the Ministry of Finance, and 36 attacks were the Estonian parliament s, prime minister's, and general government

further been estimated that some of the attacks lasted more than 10 hours, d 95Mbps, and peaked at about million packets per second While this may e a lot, other attacks considered "big" by security experts usually peak at

oS attacks have been launched against governments for various s including political or ideological ones. For example, Swedish ent websites were attacked in the summer of 2006 as a protest the country's anti-piracy measures. More recent events in Estonia sed an interesting discussion on what a cyber attack of this nature or countries.[5]

cks on the DNS

cks using **"recursive resolvers"**. While these attacks use recursive s as their force-multiplier, they need not be directed at DNS targets lthough that's where they do the most damage. They can just as se the DNS to conduct DDoS attacks against other targets. This type k uses the DNS as a weapon against something else, whereas the against the DNS root servers, described above, use something else as n against the DNS.

se attacks are often possible due to poor configuration of an ation's DNS server, which allows it to service DNS requests from re on the Internet – not just from its own network. Recursive DNS are indirectly related to malware only in so far as they use a small of compromised information systems to send fake DNS requests. other forms of DDoS attack, it does not depend on a large number of work or be more effective. It is important to note that the purpose of e or amplification attacks is not to deny service to the DNS system ut rather to the DNS server of a single organisation. This has the of making the IP routing unresolved to the entity's domain name and outbound DNS requests for the organisation difficult because of the ption of resources at the organisation's DNS server. Although is not always directly involved, it is also an example of how a user 's configuration can have a negative impact on others' security.

main-name tasting. Another trend in which malware may be ed, but not directly involved, is the practice of domain name tasting. name tasting is the practice of adding a grace period[6] to the ion of domain names so that the registrants can test the profit l of the domain names. During this period, registrants conduct a efit analysis to determine if the tested domain names return enough o offset the registration fee paid to the registry over the course of the

ard was declined. The process has been exploited to permit the ion of domain names in bulk. Although difficult to prove, it is likely e "tasted" domains are used to distribute malware.

Box 2.2 A closer look at DNS

Domain Name System (DNS) is like an address book for the Internet. It sers to navigate, send and receive information over the Internet. Every er connected to the Internet uses a unique address which is a string of s called an "IP address" (IP stands for 'Internet Protocol').[7] Because IP es are difficult to remember, the DNS makes using the Internet easier by g a familiar string of letters (called the "domain name") to be used instead umeric IP address. For example, instead of typing 193.51.65.37, users can ww.oecd.org. It is a "mnemonic" device that makes the addresses for er hosts easier to remember.

omain name consists of various parts, the top-level domain (TLDs) and the nains. TLDs are the names at the top of the DNS naming hierarchy. nly used generic TLDs include .com, .net, .edu, etc. Also, there are y 244 country code TLDs (ccTLDs), such as .jp, .au, .de, etc. The strator for a TLD controls the second-level names which are recognised in D. The administrators of the "root domain" or "root zone" control what re recognised by the DNS.

root servers contain the IP addresses of all the TLD registries – both the registries such as .com, .org, etc. and the 244 country-specific registries s .fr (France), .cn (China), etc. This is critical information. If the ation is not 100% correct or if it is ambiguous, it might not be possible to key service on the Internet. In DNS, the information must be unique and ic.

data in the DNS is stored in hierarchical and widely distributed sets of es known as "name servers", which are queried by "resolvers". Resolvers n part of the operating system or software on the user's computer. They d to respond to a user's request to resolve a domain name – that is, to find responding IP address.

Internet Corporation for Assigned Names and Numbers.
nn.org/en/general/glossary.htm.

modify data

output (screen or printer), and storage (USB, hard disk or memory). once a system is compromised, the integrity (*i.e.* trustworthiness) of re system can no longer be relied upon. Attacks on integrity are y a precursor to other attacks, such as the theft of sensitive data, or feature of an attack on authentication. However, attacks on integrity an end goal. For example, modifying entries in a database to e fraud or deleting a company's customer database for commercial e or modifying settings on a SCADA system used for gas ion may be designed to lead to a harmful malfunction of that

other currently popular attack that modifies data is compromising a and inserting an Iframe[9], which infects regular visitors to that site. can be inserted into legitimate websites to link to malware hosting t can then compromise the user.

dentity

re are substantial differences between statistical information l on ID theft by public authorities for policy purposes versus that l by private businesses for commercial purposes. Some sources e that the scale of ID theft has gone down in the past years, resulting ing consumer confidence. In contrast, other sources advance figures g an increase in ID theft. Furthermore, some financial institutions, ay that the costs are relatively modest, are not willing to reveal their nancial losses. On the other hand, other private bodies advance reflecting an increase in ID theft. To further complicate the pe, some financial institutions even claim that none of their rs has ever been affected by a phishing attack (Devillard, 2006). re some data to illustrate the debate around ID theft.

In 2006, the Netcraft toolbar, an anti-phishing tool developed by the Netcraft toolbar Community[10], blocked more than 609 000 confirmed phishing URLs, a substantive jump from 41 000 only in 2005 (Netcraft Toolbar Community, 2007). Netcraft views this dramatic surge, mainly concentrated in November- December 2006, as the result of recent techniques implemented by phishers to automate and propagate networks of spoof pages, enabling the rapid deployment of entire networks of phishing sites on cracked web

increase since September 2006. However, in its December 2006 report the APWG notes a decrease in the number of new phishing sites (which dropped to 28 531) (APWG, 2006b).

The US Federal Trade Commission reported in 2003 that ID theft affected approximately 10 million Americans each year (US FTC, 2003).[12] In 2007, another report found that ID fraud had fallen about 12% from USD 55 7 billion to 49 3 billion (Javelin Research and Strategy, 2007)

However, the Javelin report was criticised and regarded as trying to persuade the opinion that "business are doing an adequate job in protecting consumers' personal information and that the onus in on consumers to better protect themselves" (Shin, 2007). A recent McAfee survey noted this discrepancy, considering Javelin's percentages as "surprisingly low" and comparing them to Gartner statistics, which, in contrast, in 2007, counted 15 million of Americans as victims of ID theft (McAfee, 2007)

ingle and multi-factor authentication

acks on single-factor authentication, such as a username and reusable d, using malware are widespread and highly effective. Such attacks, cks on integrity, are precursors to stealing information of value via the compromised computer. Single-factor credentials for computer s, online banking accounts, virtual private network (VPN) remote nd the like are all vulnerable to capture via keyboard, screen, mouse protected storage (or similar areas) within the information system then easily replayed by an attacker to access the relevant accounts or

acks on some forms of multi-factor authentication are also possible ve occurred. For example, most simple forms of multi-factor cation, including the use of a hardware token which generates a one- assword and challenge-response with a short time to live are ble to malware attack. For example, a Trojan, once installed on the omputer simply waits for the user to establish a legitimate login with their bank using their multi-factor credentials. Then the Trojan s a funds transfer in the background without the user's authorisation

m to successfully authenticate to E-gold's website, then creating a browser session, and using various spoofing tricks to empty the account. Because the stealing and spoofing started after the cation is completed, it circumvented any authentication that was put While the e-gold Trojan did not attack multi-factor authentication it was an early example of malware able to transfer funds in the und after the user legitimately logs on to their e-gold account which ave defeated any type of multi-factor logon authentication that did implement transaction signing (Stewart, 2004)

Box 2.3 The two-factor token attack

ght variation of the two-factor token attack involving a hybrid phishing lware attack, reportedly targeted ABN AMRO's online banking customers . The attacker sent potential victims an e-mail purporting to be from their e ABN AMRO) If recipients opened an attachment to the e-mail e was installed on their computers without their knowledge When the ers next visited their banking site, the malware redirected them to the -controlled website that requested their security details, (i.e their PIN) -time password (OTP) generated by the hardware token. As soon as the s received these details they were able to log into the customer's account real ABN Amro site, before the expiry of the automatically generated enabling them to transfer the customer's money As single-factor ication for high value transactions are replaced by multi-factor ication, this type of attack will become more commonplace

Outlaw.com (2007) and The Registar (2007)

ligital certificates and secure socket layer (SSL)

ital certificates and Secure Socket Layer (SSL) connections are often protect the confidentiality and integrity of data sent over the Internet verify the authenticity of the remote host (most commonly to cate a remote server) While these protections are useful, they do not security at the end points of a transaction, but generally only the in between. While an SSL session is established, data needs to be d and decrypted as data are transferred back and forth between the its When a users' machine has been compromised by malware[14], the ng sent can be captured *before* encryption occurs – and for data – *after* it has been decrypted Efforts to provide a higher level of

Errors and warnings due to invalid SSL certificates are frequently highly technical in nature and therefore confusing to users.

According to one usability study performed, consumers most often ignore the absence of an SSL connection before entering personal data, or ignore warnings provided (Dhamija, 2007).

When organisations use self-signed certificates, "untrusted signer" warnings may be displayed and generate confusion for users.

In some cases, malicious site operators have been able to obtain legitimate SSL certificates from Certificate Authorities (Krebs, 2006).[15]

Box 2.4 The problem with digital certificates and SSL

gital certificate[16] is a mechanism to establish the credentials of a person or onducting business or transactions online. It is often used within SSL[17] ed sessions. The use of digital certificates within SSL protected sessions is is of building trust and confidence in e-commerce and e-government ions. However, some forms of malware when installed on a user's er can wait for a legitimate SSL session to be established with a particular , for example a specific online banking site, and then inject HTML code browser interface before the legitimate remote web site page renders on 's computer.

has the effect of changing the content and appearance of the web page hough the remote site has not been modified), while the user's computer intains a valid SSL connection with the remote host. A check of the SSL ertificate, by the user, will show that it is a valid certificate for the remote hat the user sees on the screen and the data the user is prompted to input, r, differ from the contents of the legitimate remote site.

manipulating the compromised computer's browser interface, attackers virtually impossible for users to know whether or not they have a secure ion with a legitimate remote host – and by inference – whether what they he browser window is the content of the legitimate remote host. Therefore, of digital certificates within SSL-protected sessions, as a means of verifying the identity of a remote web domain, has been fundamentally ined.[18]

s are perpetrated

cess and restore the data.[19] Although this type of malware is not as it as other types of malware, there were several high profile cases in at raised attention around the issue (Sophos, 2007a). Such attacks, y deny the user/owner access to their own data, but harm the ntiality and integrity of that data by the attacker's unauthorised o it and encryption of it.

Box 2.5 A ransom example: the Arhiveus

ne 2006, a Trojan horse attacked files in Microsoft Windows users' "My ents". The files were then encrypted so users could not access them paying a ransom in return for the restoration of the files.

n users tried to access their files, they were directed to a file containing ions on how to recover the data. The instructions began:

TRUCTIONS HOW TO GET YOUR FILES BACK READ CAREFULLY OU DO NOT UNDERSTAND - READ AGAIN

s is the automated report generated by auto archiving software

r computer caught our software while browsing illegal porn pages, all r documents, text files, databases in the folder My Documents was hived with long password

cannot guess the password for your archived files password length is e than 30 symbols that makes all password recovery programmes fail to e force it (guess password by trying all possible combinations)

not try to search for a programme that encrypted your information - it ply does not exist in your hard disk anymore. Reporting to police about a will not help you, they do not know the password. Reporting somewhere ut our email account will not help you to restore files. Moreover, you and r people will lose contact with us, and consequently all the encrypted rmation.

many of these cases the attacker encrypts files such as personal raphs, letters, household budgets and other content. To retrieve their data, ere required to enter a 30 character password which they were told would lable after making purchases from one of three online drug stores.

Sophos (2007b) 'Security Threat Report Update July 2007", *phos.com/security/whitepapers/*, accessed 12 December 2007

the UK's public and private critical information infrastructure
rojans were assessed to be seeking covert gathering and transmitting
leged information (NISCC, 2005) Malware of this sort can also be
companies and other organisations to gather information about their
tors as demonstrated by the below example

Box 2.6 The case of Michael and Ruth Haephrati

larch of 2006, Michael and Ruth Haephrati were extradited to Israel from
where they were charged with creating and distributing a Trojan used to
t industrial espionage against some of the biggest companies in Israel
l Haephrati is said to have developed and refined the programme while his
Ruth, managed business dealings with several private investigation
ies which bought it and installed it on the computers of their clients'
ntors Specifically, the Trojan horse is believed to have been used to spy
Rani Rahav public relations agency (whose clients include Israel s second
mobile phone operator, Partner Communications), and the HOT cable
on group Another alleged victim was Champion Motors, who import
nd Volkswagen motor vehicles

Brier-Haephrati was formally charged with aggravated fraud, unlawful
er access, virus insertion, installing tapping equipment, invasion of
, managing an unlawful database, and conspiracy to commit a crime
l Haephrati was charged with lesser offenses as the prosecution regarded
Ruth s assistant because his job was only to perfect the programme and
to the needs of specific clients

Messagelabs (2006) and Sophos (2006c)

g information

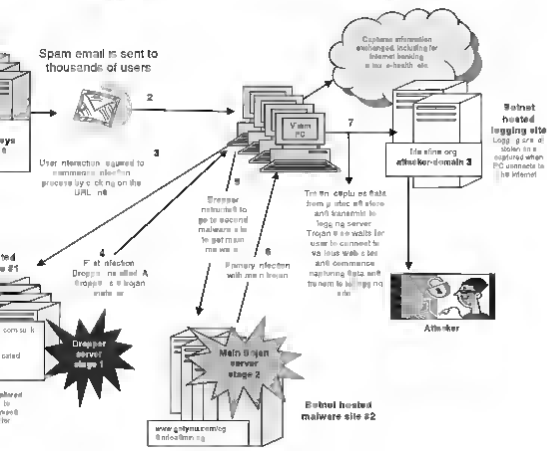
r the past five years, information theft, and in particular online
(ID) theft[20], has been an increasing concern to business,
ients, and individuals Although malware does not always play a
ole[21], ID theft *directly* using malware has become increasingly
n with the rise of backdoor Trojans and other stealthy programmes
e on a computer system and capture information covertly

llustrated in Figure 2 I, online ID theft attacks using malware can be
and can use multiple Internet servers to distribute spam and
, compromise users' information systems, and then log the stolen
nother website controlled by the attacker or send it to the attacker's

use of multiple domain names and multiple hosts or bots (and their ed IP addresses) is designed to increase the time available for g the sensitive information and reduce the effectiveness of efforts by organisations (such as banks), CSIRTs and ISPs to shut down nt sites. Under the domain name system (DNS), attackers are able to and easily change their DNS tables[23] to reassign a new IP addresses ulent web and logging sites operating under a particular domain.[24]

effect is that as one IP address is closed down, it is trivial for the emain active under another IP address in the attacker's DNS table mple, in a recent case IP addresses operating under a single domain hanged on an automated basis every 30 minutes, and newer DNS have made it possible to reduce this time to five minutes or less. rs may use legitimate existing domains to host their attacks, or specially created fraudulent domains. The only viable mitigation to the latter situation is to seek de-registration of the domain RT, 2006).

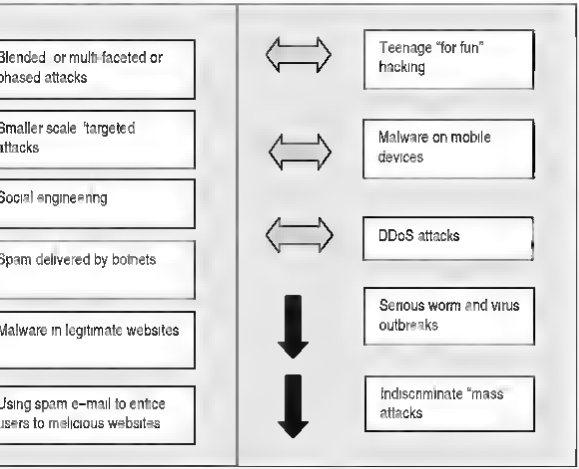
Figure 2.1 Online ID theft attack system involving malware



ack trends

dynamic nature of malware keeps most security experts constantly ookout for new types of malware and new vectors for attack. Due to plex technical nature of malware, it is helpful to examine overall ends to better understand how attacks using malware are evolving. ntioned previously, the use of malware is becoming more cated and targeted. Attackers are using increasingly deceptive social ring techniques to entice users to seemingly legitimate web pages actually infected and/or compromised with malware. Figure 2.2 es the types of attack that seem to be on the increase, those that are out of favour, and those for which the trend remains unclear or not .

Figure 2.2 General attack trends



alware attacks

gin refers to both where the attackers who launch the attack are based ere the computer systems that actually attack the targeted system are In most cases, it is easy to see where the attacking computer are hosted based on their Internet protocol or "IP" addresses, but ot usually sufficient to identify the person responsible for launching ck. For example, "spoofing" is a technique designed to deceive an med person about the origin of, typically, an e-mail or a website.[25]

reover, rarely is the attacker located in the same geographic region as cking hosts It is common practice among cybercriminals[26] to use mised computers (and to a lesser extent anonymous proxies[27]) hosted eign legal jurisdiction to launch their attacks This protects their and provides additional computing resources beyond what they therwise afford Criminals are acutely aware of the significant ional impediments that hinder or even prevent cybercrime ations from being conducted if the crimes are sourced onally

ware is now spread around the world and rankings[28] tend to show whole host of countries across the developed and the developing re home to online criminals using malware Although attacks ng from one country may have local targets, the predominant trend s that originate internationally relative to their targets In addition, hy may play a role depending on the end goal of the attacker For , broadband Internet speeds differ from country to country If an wishes to maximise network damage, he/she may use compromised rs located in countries where broadband is prevalent If the goal is ade service or steal information over time, the attacker may use mised computers from a variety of geographical locations phical distribution allows for increased anonymity of attacks and identification, investigation and prosecution of attackers

Figure 2.3 Malicious actors

The Innovators

ed individuals who devote their time to finding security holes in systems
ew environments to see if they are suitable for malicious code
nge
ce the challenge of overcoming existing protection measures

The Amateur Fame Seekers

s of the game with limited computing and programming skills
for media attention
eady-made tools and tricks

The Copy-Catters

be hackers and malware authors
for celebrity status in the cybercrime community
ted in recreating simple attacks

The Insiders

ntled or ex-employees, contractors and consultants
ge or theft
dvantage of inadequate security aided by privileges given to their
n the workplace

Organised Crime

motivated, highly organised, real-world cyber-crooks, Limited in
mitless in power

core of masterminds concentrated on profiteering by whichever means
rounding themselves with the human and computer resources to make

Inc (2006) 'Virtual Criminology Report 2007 Organized Crime and the Internet",
e com/us/threat_center/white_paper html

ıs actors

e the malicious actors?

anised Crime"[29] based on a recent report on criminal activity on line
portant to note, however, that there is also a whole category of actors
notivations are political or ideological rather than solely financial

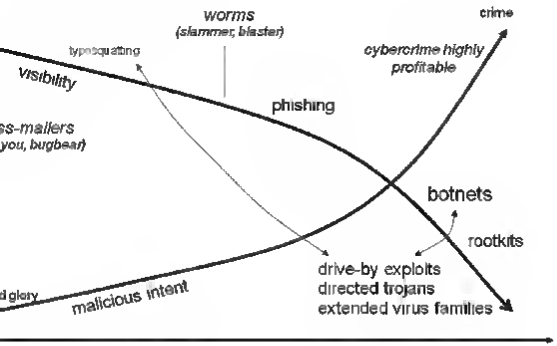
le a certain amount of crime is always "local", the vast majority of
rime crosses jurisdictional boundaries and international borders thus
g the criminals' risk of identification and prosecution. Because many
attacks are not able to be traced back to the people that conduct
is difficult to provide authoritative insight into the nature of groups
iduals involved in the proliferation of the various types of crime
r, some law enforcement and financial institutions are actively
d in monitoring and investigating the money trails arising from
nt fund transfers as a result of phishing and ID theft Trojan related
These investigations involve identification of money mules, who are
als recruited wittingly and often unwittingly by criminals, to
e illegal funds transfers from bank accounts

ure 2.4 illustrates the evolution of malware in terms of malicious
the actors showing a clear evolution from fame seeking "techies" to
s motivated by financial gain

re their capabilities and motivations?

demonstrated earlier in this report, attacks using malware are
g increasingly complex. But while the sophistication of the attacks
increase, the knowledge required to carry them out significantly
es. Although this might seem counterintuitive, it can largely be
d to the increased market for malware. The majority of today's
s are motivated adversaries who are capable of purchasing malware
urcing attacks to more sophisticated attackers

Figure 2.4 Visibility of malware vs. malicious intent



Govcert nl, *www govcert nl*

e business model

expert recently noted that "creating one's own bot and setting up a s now relatively easy. You don't need specialist knowledge, but can download the available tools or even source code" (McAfee Inc., In addition, "off-the-shelf" kits with ready-made Trojans can be nded from the Internet. Some versions are guaranteed by the authors n undetected by security defences and some even include a "service greement" by which the author guarantees, for a certain period of create new versions for the criminal once the original malware is . It has been estimated that this service can cost as little as USD 800 eLabs, 2006). In addition, many malicious services, such as botnets, lable for hire.

ware, and by extension its main propagation vector, spam[30], are ngly combined as key underpinnings of criminal techniques to make the rapidly evolving "Internet economy". Malware has evolved into narket" money-making schemes because it offers such a profitable model. Malware techniques are becoming increasingly cated, but some users continue to lack appropriate protection. anding the malware business model can help industry participants

orate espionage, or to gain access to privileged or proprietary tion or to deny access to critical information systems).

attackers continue to remain successful at launching attacks, the economy becomes self-perpetuating. Spammers, phishers, and yber criminals are becoming wealthier, and therefore have more l power to create larger engines of destruction. It is a big business, d by wealthy individuals, with multiple employees and large s of illicit cash. In addition to an increased frequency and cation of attacks, the amount of damage is significant.[31]

dern attacks demonstrate an increasing level of convergence, with a ation of spam and social engineering designed to yield the greatest profitability to the attacker. In addition, today's attacks often consist es of waves each having a specific purpose. A simple attack will aim ing up a list of valid e-mail addresses. It will be followed by e-mail harvested accounts containing viruses with a payload that makes a ystem part of a botnet. Once part of a botnet, the machines are often disseminate phishing emails which in turn produce the attack's y return.

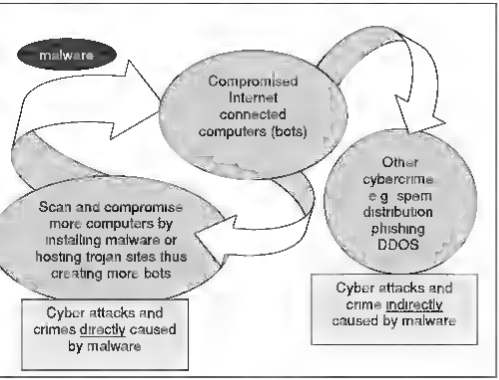
conomic rationale for malware

ail is not at an economic equilibrium between the sender and the t because it costs virtually nothing to send. All the costs of dealing am and malware are passed on to the Internet provider and the ng" recipients, who are charged for protective measures, bandwidth er connection costs, on top of the costs of repairing the computer or ost money to scams. At the same time, criminals minimise their costs treme: they pay no tax, escape the cost of running a genuine business, and mmission only to others in criminal circles worldwide and at a tively low price.

cost to malicious actors continues to decrease as freely available orage space increases. Further, the use of botnets makes it easier and eaper to send malware through email. Today's criminals often have o cheap techniques for harvesting email addresses as well as easy to malware and outsourced spamming services. Anti-detection nes are constantly evolving to make it cheaper to operate, and is actors can easily switch ISPs if their activity is detected and their

n the malware itself and the compromised computers being used to launch malware attacks are a low cost, readily available and easily ble resource. High speed Internet connections and increased dth allow for the mass creation of compromised information systems nprise a self sustaining attack system as illustrated by Figure 2.5. more, malicious actors can replace compromised information that have been disconnected or cleaned, and they can expand the of compromised information systems as the demand for resources malware and compromised information systems) for committing me also grows.

Figure 2.5 Self sustaining attack system using malware



ote: this figure shows how malware is used to create a self sustaining ource of compromised computers that serve as the backbone of licious online activity and cybercrime. Information systems connected the Internet can become infected with malware. Those information stems are then used to scan and compromise other information systems.

ying business process

underlying business processes for spam and malware largely follow e pattern.

Gathering of addresses, targeted or not, and/or developing or acquiring control of a botnet

Delivering spam, with or without malware, from other people's computers through botnets

Publishing fraudulent websites to capture users' data

his pattern, certain groups of attackers are active in the entire value tarting with the development of the malware and performing the of the spam and/or malware, all the way to laundering the money "clean" bank account Much of the criminal market, however, is ed into clusters of expertise with the opportunity to source partners , primarily through Internet Relay Chat (IRC) channels, ound bulletin boards, and online forums

minals develop, maintain and sell malware, botnets, spam ssion software, CDs full of addresses harvested from web pages, lists proxy servers and lists of open simple mail transfer protocol [32] relays The lists of addresses or controls of a botnet are then ut or sold These lists are often inexpensive at around USD 100 for on addresses An entire online criminal operation could be carried ttle or no cost, the only hard costs are various "utilities" such as lth, Internet connection, e-mail addresses, or web hosting, and even n be financed illegally.

le the use of malware to facilitate cybercrime, particularly crimes ed by illicit financial gain, has increased, the money made through is online activity has become increasingly difficult to trace As in al criminal investigations, tracing where the money goes by g the cash flows could provide essential information on the s However the victims of online malicious activity are increasingly pay by wire transfers (46% of online scams transactions in the US), followed by card payment (28%), both much preferred for their nd the potential to mask tracks easily, by comparison with cheques which now represent less than 10% of the payments.[33] These types ents are fast and can be made almost anonymously through the use ple financial accounts across borders Alternative payments systems 'e-Gold' or PayPal used by criminals further down the chain make it ore difficult to trace financial movements Users of these online t services can open an account using a fraudulent name and deploy a

Notes

e "Indirect attacks on the DNS" below for further information on types attacks.

is also possible to cause a denial of service in a network device or plication by exploiting vulnerabilities in an operating system or plication software. For example, this could be accomplished by an tacker sending specially crafted packets to the device or application here the vulnerability exists. DOS attacks of this type can be rectified, owever, by applying the software or firmware patch, or implementing me other work-around. In the case of flood attacks, the ability to itigate is more difficult and protracted and hence the impact is otentially more serious.

e Chapter 1, "The Malware Internet Botnets" section, for a mprehensive discussion of bots and botnets.

n Internet exchange point (IX or IXP) is a physical infrastructure that lows different Internet Service Providers (ISPs) to exchange Internet affic between their networks by means of mutual peering agreements, hich allow traffic to be exchanged without cost. IXPs reduce the portion an ISP's traffic which must be delivered via their upstream transit oviders, thereby reducing the Average Per-Bit Delivery cost of their rvice. Furthermore, IXPs improve routing efficiency and fault-lerance.

or example, a senior official was quoted by *The Economist* saying "If a ember State's communications centre is attacked with a missile, you call an act of war. So what do you call it if the same installation is disabled ith a cyber-attack?", see *The Economist* (2007), "A cyber riot", 10 ay.

he Add Grace Period (AGP) refers to a specified number of calendar ys following a Registry operation in which a domain action may be versed and a credit may be issued to a registrar. AGP is typically the ve day period following the initial registration of a domain name.

he Internet Protocol (IP) allows large, geographically diverse and

his is a theoretical proposition only The authors are not aware that such ber attacks have occurred involving the use of malware

Frame" is the hybrid of *inline frame*, and describes an HTML element hich makes it possible to embed another HTML document inside the ain document IFrames are commonly used to insert content (for stance an advertisement) from another website into the current page

he Netcraft toolbar Community is a digital neighbourhood watch heme in which expert members act to defend all Internet users against ishing frauds Once the first recipients of a phishing e-mail have ported the target URL, it is blocked for toolbar users who subsequently cess that same URL

hese packages, known broadly as Rockphish or R11, each included ozens of sites aimed at spoofing major banks

his includes all types of ID Theft, online and offline

Gold is a 'digital currency', but which is backed by real gold and silver ored in banks in Europe and the Middle-East E-Gold can be used as a isted third party intermediary whereby the money is transferred only ce the product or service bought has been received

ost (if not all) Trojan variants being used for illicit financial gain have e ability to capture data transmitted during an SSL session – not just ose which also include HTML injection functionality

certificate authority is an entity, such as Verisign, that issues rtificates

digital certificate is a means of authenticating an identity for an entity hen doing business or other transactions on the web or on line Digital rtificates exist as part of public key infrastructures (PKI) PKI uses blic key cryptography and an associated hierarchical infrastructure of ot Certification Authorities (CAs) and Registry Authorities to process quests for, issue and revoke certificates Even when a digital certificate valid, all valid certificates should not be trusted equally Some rtificates are self-signed and hence have no independent third party to rify that they are a legitimate business entity or own a particular domain d others, which may be issued by a CA, have only low assurance levels, the CA has provided only very basic checking to verify that the entity who it is claiming to be A certificate contains the entity's name, a rial number, certificate expiration dates, a copy of the certificate lder's public key (used for encrypting messages and verifying digital

SL is a cryptographic protocol used to provide secure communications
the Internet, for such things as web browsing, e-mail, Internet faxing,
stant messaging and other data transfers

ore recent versions of the Haxdoor Trojan also have the ability to use
TML injection See AusCERT (2006)

has been assessed that such attacks are not likely to gain popularity as
y organisation with a basic level of preparedness should have back-up
pies of their data available However, it may also be that individuals are
t aware of this risk, or simply lack basic security education to protect
emselves from malware

e OECD (2008b), where Identity Theft is defined as the unlawful
nsfer, possession, or misuse of personal information with the intent to
mmit, or in connection with, a fraud or other crime

entity theft attacks most often use social engineering techniques to
nvince the user to necessarily disclose information to what they assume
a trusted source This technique, known as Phishing, does not *directly*
ly on the use of malware to work It uses deceptive or "spoofed" e-mails
d fraudulent websites impersonating brand names of banks, e-retailers
d credit card companies to deceive Internet users into revealing
rsonal information However, as many phishing attacks are launched
om spam emails sent from botnets, malware is *indirectly* involved as it
used to create botnets which are in turn used to send the spam e-mail
ed in phishing attacks Malware would be *directly* implicated when the
am e-mails contained embedded malware or a link to a website where
alware would be automatically downloaded

ns is a technique known as "fast flux"

DNS table provides a record of domain names and matching IP
dresses

e previous sections of Chapter 2 for a discussion on attacks using the
NS and attacks against the DNS

hen spoofing is used, identifying the source IP address of an e-mail or
ebsite is usually a futile effort It is also possible to spoof the source IP
dress of an IPv4 datagram, thereby making real identification of the
urce IP address much more difficult It should be noted that this is often
t required for an attack to succeed or can be counter-productive for the
tacker if the objective is to steal data from a computer The use of
onymising technologies could pose a more serious problem for

ere we refer to cybercriminals who are conducting attacks full-time for
icit financial gain and may have an area of specialisation or be involved
a variety of business lines such as phishing, Trojans, spam distribution,
ckfraud, malware development, etc.

computer networks, a proxy server is a server (a computer system or an
plication programme) which services the requests of its clients by
rwarding requests to other servers. A client connects to the proxy
rver, requesting some service, such as a file, connection, web page, or
her resource, available from a different server. The proxy server
ovides the resource by connecting to the specified server and requesting
e service on behalf of the client. A proxy server that removes
entifying information from the client's requests for the purpose of
onymity is called an anonymising proxy server or anonymiser.

r example, see Symantec (2007) p. 9.

Organised crime" is used loosely in this context and often refers to a
oup of profit-motivated criminals who trade services with one another
an open marketplace.

discussed previously in this paper, not all spam contains malware
owever the majority of spam is sent from information systems that have
en compromised by malware.

e Chapter 3, "Malware: Why Should We Be Concerned?" for a
scussion of the impacts from malware.

mple Mail Transfer Protocol (SMTP) is the de facto standard for e-mail
nsmissions across the Internet.

nited States National Consumer League / National Fraud Information
enter (2006), p. 2.

ter 3. Malware: Why Should We Be Concerned?

growth of malware, and the increasingly inventive ways in which it
used to steal personal data, conduct espionage, harm government
ness operations, or deny user access to information and services, is a
lly serious threat to the Internet economy, to the ability to further e-
ent for citizen services, to individual's online social activities, and
al security

abling factors

capabilities of malware make it a prevalent "cybercriminal tool".
r, broader economic and social factors may contribute to its
d occurrences and the robust state of the malware economy. The
g describes some of those factors which, while they bring important
to society, also facilitate the existence and promulgation of

and Internet and its users

005, the International Telecommunication Union estimated 216 708
xed" broadband Internet subscribers in the world (ITU, 2007).
nore, it is generally agreed that there are an average of 1billion
users in the world today. As the number of subscribers and users
s, so does the number of available targets for malware. The
d prevalence of high speed Internet and the availability of
nd wireless connections make it easy for malicious actors to
ully carry out attacks as they can compromise computers at faster
se the bandwidth to send massive amounts of spam and conduct
ttacks. Furthermore, these "always on" connections allow malicious

important to note that while broadband technologies are an enabling
it is the behaviours associated with these technologies that are
natic. For example, people often fail to adopt appropriate security
s when using broadband technologies and therefore leave their
ion open without the appropriate security software installed [1]

ore services available online

st governments, consumers and businesses depend on the Internet to
their daily business. In 2004, the OECD found that, in most OECD
s, over 90% of businesses with 250 or more employees had access
nternet. Firms with 50 to 249 employees also had very high rates of
OECD, 2005). Home users rely on the Internet for their day to day
s including shopping, banking or simply exchanging information
ducting e-government and e-commerce transactions. As the amount
services continues to increase, so does the likely community of
cessing these services on line. This in turn increases the available
for attack or exploitation which provides further incentive for
s to conduct malicious activity.

ng system and software vulnerabilities

more vulnerable the technology, the more likely it is to be
ble through malware. For example, the security firm Symantec
a 12% increase in the number of known vulnerabilities from the
f of 2006 (January-June 2006) to the second half (June-December
hich they largely attribute to the continued growth of vulnerabilities
applications (Symantec, 2007). Microsoft also reported an increase
y 2 000 disclosed vulnerabilities from 2005 to 2006. The increase in
ilities corresponds to an increase in incidents. Microsoft reported an
in the number of machines disinfected by its Malicious Software
l Tool from less than 4 million at the beginning of 2005 to more
million at the end of 2006 (Microsoft, 2006b).

important to note that the absence of known *reported* vulnerabilities
tware product does not necessarily make that product more secure
e that has known reported vulnerabilities – it may simply be that
ffort has not been expended to find them. In addition, tools that find
ploit vulnerabilities are improving, companies are doing more

target average Internet user

the reliance of home users and small to medium-sized enterprises on the Internet increases, so do the malware threats they face. ers and business are increasingly exposed to a new range of ., targeted attacks that use malware to steal their personal and l information.

ny Internet users are not adequately informed about how they can manage their information systems. This lack of awareness and ent action or inaction contributes to the increasing prevalence of . Most malware requires some form of user action or acceptance to te. Recent surveys from various organisations show that while more re taking measures to protect their information systems, a large ge of the population lacks basic protective measures. For example, a port commissioned by the Australian Government, *Trust and Growth Online Environment*, found that only one in seven computers in a uses a firewall and about one in three uses up-to-date virus on software (OECD, 2007b). After hearing descriptions of re" and "adware," 43% of Internet users, or about 59 million n adults, said they had had one of these programs on their home r (Brendler, 2007).

European Commission's Eurobarometer E-communications old survey, observed an increase in consumer concerns about spam ases in 2006 (European Commission, 2007). For some EU Member up to 45% of consumers had experienced significant problems. In the cases, the computer performance decreased significantly, in 27% cases a breakdown was observed. In the same survey, 19% of ers had no protection system at all on their computers. Other data ggests that home users are the most targeted of all the sectors ing for 93% of all targeted attacks[2] and thus highlighting that weak urity is one important enabler of malware (Symantec, 2007).

malware

nany cases, the consequences of inadequate security measures are l" or borne by others in society. For example, if one user's computer ed to a network or the Internet is inadequately protected and

le many attack trends are increasing, it is nevertheless unclear how ends relate to the overall damage caused by malware. Detecting a umber of Trojan variants does not necessarily mean that there is mage. It could also be a response to improved security defenses y, signalling that large-scale botnets are shrinking in size does not ily mean that the counter measures are effective. It might be that s have found smaller and more focused botnets to be more le. In short, because malicious attack trends are highly dynamic, it is to draw reliable conclusions from them regarding economic

vever, considering the growing proportion of compromised tion systems connected to the Internet in any single country and the ng challenges to detect and remove malware, the impacts of malware ty are, in all probability, rising as a result

ial impacts – sample data

ough precise data on online criminal activity and the associated l losses are difficult to collect, it is generally accepted that malware tes significantly to these losses.[3] Further, where data on cybercrime conomic impact are available, businesses and governments are often t to share it publicly

association of banks in the United Kingdom estimated the direct aused by malware to its member organisations at GBP 12.2 M in BP 23.2 M in 2005, and GBP 33.5 M in 2006, an increase of 90% 04 and 44% from 2005 (Whittaker, 2007). It is important to note that rect losses are not fully representative of the actual financial impact do not measure diminished customer trust in online transactions, loss ation, impact on the brand, and other indirect and opportunity costs challenging to quantify. Likewise, they do not include costs, such as xpenses for analysing malware, repairing, and cleansing infected s, costs associated with the procurement of security tools (such as s and anti-malware software), or loss of productivity caused by the of employees to interact with a system when affected by an attack

recent survey of 52 information technology professionals and rs estimated a slight decline in the direct damages associated with , from EUR 12.2 billion in 2004, to EUR 10 billion in 2005, to EUR

ed the annual loss to United States businesses at USD 67 2 billion
vernment Accountability Office, 2007)

ough the malware-related costs of security measures are considered
ary, estimates provided by market participants in the empirical study
d in Part II of this book ranged from 6-10% of the capital cost of
ns (Van Eeten, 2008) No clear estimates of the effects of malware
ating expenses were available, although the study found that most
ations did experience such effects (see Part II, "Survey Results on the
f Malware") There was evidence throughout the empirical research
rn that such effects are important, although no specific indication as
magnitude is available

cost to individual consumers may be even more difficult to
, however, it is likely significant One example is the United States
onsumers paid as much USD 7 8 billion over two years to repair or
information systems infected with viruses and spyware (Brendler,

le most of the data are not comparable across studies, and the
are often limited in scope, they do illustrate the magnitude of the
l impact, for both businesses and consumers, resulting from
Also, the collective public costs of fighting malware – ranging
costs of maintaining public-private monitoring organisations, to the
public education campaigns and law enforcement – add to these
osts Finally, there are the potentially high indirect costs of malware
rm of slower migration to efficiency enhancing forms of electronic
ons The research study presented in Part II of this report indicates
direct and indirect costs of malware could be a double-digit
ge of the revenues of participants in the information and
nications market

pact on market participants

following briefly illustrates how some key market participants are
by malware (Eeten and Bauer, 2008)

t Service Providers (ISPs)

the costs and revenues of ISPs, and hence their profitability, are

botnets generating massive amounts of spam, if left uncontrolled, pportunity costs to the ISP

level of these opportunity costs depends on the capacity utilisation xisting network. If the network has significant spare capacity, the nity costs of additional traffic to the ISP will be low. However, if the is near capacity utilisation, the opportunity costs may be significant mental malware-induced traffic may crowd out other traffic in the in and require additional investment in network facilities, in ar routers and transmission capacity, in the medium and long run.

ware may also affect an ISP indirectly via reduced revenues if its ame or customer reputation suffers, for example, because of ting and reduced connectivity. ISPs will invest in preventative s reducing malware, such as filters for incoming traffic or gy that enable them to quarantine infected customers, only if the ss than the direct and indirect cost inflicted by malware.

nic-commerce (E-commerce) companies

ommerce companies are affected by malware in a variety of ways. ave to deal with DDoS attacks, often requiring them to buy more ervices from their ISPs so as to protect the availability of their . Furthermore, malware has been used to capture confidential r data, such as the credit card information registered with rs' accounts with e-commerce companies. Some sophisticated forms are have been able to defeat the security measures of online banking t rely on so-called multi-factor authentication – *i.e.* on more than login credentials.

n if customer information does not immediately allow access to l resources, it can be used to personalise phishing e-mails that try to stomers into revealing financial information. There are also cases he malware is located on the servers of e-commerce companies, are unaware that their website hosts malicious content that is ed to its visitors. Typically, it is the e-commerce customers ves that are harmed, though directly or indirectly the e-commerce y may also be affected. Financial service providers often compensate for their customers. For other companies there can be reputation

ese vulnerabilities does not impact the software vendors directly, t may have reputation effects and require costly response measures ing, testing and applying vulnerability patches is costly, not only on of the vendor, but also for its customers

ware developers typically face difficult development trade-offs security, openness of software as a platform, user friendliness, and ment costs Investments in security may delay time to market and ave additional opportunity cost in the form of lost first-mover ges On the other hand, if reputation affects work, software vendors roducts have a reputation of poor security may experience costs in of lost revenues These effects are mitigated, however, by the fact ny software markets tend to have dominant firms and thus lock-in rs to specific products

name registrars

istrars have become part of the security ecosystem Their business s and policies affect the costs of malware and of the criminal models built around it Registrars may derive additional revenues omain name registrations, even if they are related to malware, but not incur any specific direct costs Nonetheless, if their domains are ed with malicious activity, it may result in an increasing number of and informal abuse notifications Dealing with such abuse ions is costly, requiring registrars to commit and train staff ling domains may also result in legal liabilities

hermore, many registrars may be ill-equipped to deal with malware ration requests Malware domain de-registrations can be very to process compared to, for example, phishing domain de- ions, which are normally a clear breach of trademark or copyright xperts report that registrar abuse handling teams will often cite ent evidence to process a de-registration request, although evidence nt for many incident response teams has been provided Because of of legal action where a legitimate domain would be incorrectly de- d, registrars often prefer to support their customer rather than the nant

of the economic costs that registrars face is proving the identity of uts Certain domain spaces (com au, for example), require strict tests

rs

l users form the most diverse group of players, ranging from home o large corporations or governmental organisations. End user s, from home PCs to corporate web servers, are the typical target of . The economic impact of these infected computers is distributed he whole value system. Some of the impact is suffered by other layers, not by the owners of the infected machines, although there is lware directly impacting the owners, for example by stealing information from the compromised machine.

n of trust and confidence

iety's heavy reliance on information systems makes the ences of the failure or compromise of those systems potentially . Malware is an effective and efficient means for attackers to mise large numbers of information systems, which cumulatively has ntial to undermine and erode society's ability to trust the integrity fidentiality of information traversing these systems. The failure to adequate protection for the confidentiality and integrity of online ions may have implications for governments, businesses and ers. For example, electronic government (e-government) services, online filing for taxes or benefits, are likely to include personal data ompromised could be used to commit fraud. Information systems in isinesses or large public and private sector organisations might be access such e-government or electronic commerce (e-commerce)

nature of malware is such that it is not possible to trust the ntiality or integrity of data submitted or accessed by any computer mpromised by malware. It is often difficult to readily distinguish a mised host from one that is not compromised and, as a result, in an ment like the Internet, in which malware has taken hold, connections fected hosts must be treated as potentially suspect. Therefore, the o have trust and confidence in online transactions can be further because traditional mechanisms for building trust and confidence in rmation economy such as authentication, encryption and digital tes can also be subverted, bypassed or manipulated by malware.[6]

ecent years, a number of surveys have been conducted which show

, thus enhancing the economic benefits and efficiencies expected
use of these platforms.

re are other studies, however, which show that the convenience and
cy of the online channel is driving growth in participation in e-
ce and e-banking despite these concerns. In 2006, RSA Security
ed the first Internet Confidence Index designed to measure changes
and European confidence in secure online transactions among
ers and businesses (RSA Security, 2006). At the time, the annual
ased on data gathered from business and consumer audiences in the
States, the United Kingdom, Germany and France, revealed that the
ess to transact online was on average outpacing trust and that both
es and consumers were absorbing the risks in order to reap the
of online transactions.

se two seemingly contradictory pieces of evidence point out that the
impact of trust is not yet adequately understood and that indeed it is
to measure consumer trust and confidence in the online
ment. However, empirical evidence reveals that e-commerce
es benefit greatly from the ability to conduct business online.[8]
e estimated efficiency gains in the financial sector, for example, the
ings associated with the enormous volume of transactions translates
ery powerful incentive to move as much volume of these services as
online. Repeatedly in the study, e-commerce companies indicated
rity investment levels were much higher than justified by the direct
ften by one or two orders of magnitude (Eeten and Bauer, 2008).
direct losses are not seen as indicative of the overall problem. It
e much more devastating, for example, if online fraud eroded
r trust or slowed down the uptake of online financial services.

critical information infrastructures

ical infrastructures at the basis of our society, such as power grids or
lants, are now often dependent upon the functioning of underlying
d networks for their instrumentation and control. Most industrial
systems that both monitor and control critical processes were not
d with security in mind, let alone for a globally networked
ment, but are now increasingly being connected, directly or
y (through corporate networks), to the Internet and therefore face a

potential to impact the public and private sectors and society as a

re have been a few cases where attacks using malware have directly ectly affected critical information infrastructure. For example, in malicious hackers used a Trojan to take control of a gas pipeline run orom (Denning, 2000). In January 2003 the "Slammer" worm, which major problems for IT systems around the world, penetrated the monitoring system at a US nuclear plant for nearly five hours n, 2003). The US Nuclear Regulatory Commission investigated the and found that a contractor established an unprotected computer ion to its corporate network, through which the worm successfully the plant's network (US Nuclear Regulatory Commission, 2003). ecently, the United States indicted James Brewer for operating a of over 10,000 computers across the world, including computers at Cook County Bureau of Health Services (CCBHS). The malware he infected computers to, among other things, repeatedly freeze or vithout notice, thereby causing significant delays in the provision of services and access to data by CCBHS staff.[9]

hough governments are often reluctant to disclose instances of attack the critical infrastructure, it is apparent that protecting the tion systems that support the critical infrastructure has become ngly important.[10] Despite only a few reported cases, it is widely ood that critical information systems are vulnerable to attack. For , although the 2003 blackout in the northeast US and Canada was d to a software failure, analysis of the incident demonstrated that the were vulnerable to electronic attack, including through the use of .[11]

o fighting malware

ecting against, detecting and responding to malware has become ngly complex as malware and the underlying criminal activity which rts are rapidly evolving and taking advantage of the global nature of rnet. Many organisations and individuals do not have the resources, expertise to prevent and/or respond effectively to malware attacks associated secondary crimes which flow from those attacks such as theft, fraud and DDoS. In addition, the scope of one organisation's

and finding ways to block them, but notes that this is almost an
ble task, with about 200 new samples per day and growing (Greene,
Another company reported it receives an average of 15 000 files –
nany as 70 000 – per day from their product users as well as CSIRTs
ers in the security community (OECD, 2007b) When samples and
received, security companies undertake a process to determine if the
deed malicious This is done by gathering data from other vendors,
ing automated analysis, or by conducting manual analysis when
ethods fail to determine the malicious nature of the code One
estimated that each iteration of this cycle takes about 40 minutes and
y release an average of 10 updates per day (OECD, 2007b)
more, there are many security vendors who all have different insights
malware problem

t security technologies such as anti-virus or anti-spyware products
ature-based meaning they can only detect those pieces of malware
h an identifier, known as a "signature" already exists and have been
d. There is always a time lag between when new malware is released
kers into the "wild", when it is discovered, when anti-virus vendors
their signatures, and when those signatures are dated onto users and
ations' information systems Attackers actively seek to exploit this
f heightened vulnerability It is widely accepted that signature based
s such as anti-virus programs are largely insufficient to combat
complex and prevalent malware For example, one analysis[12] that
antivirus detection rates for 17 different anti-virus vendors reveals
n average, only about 48 16% of malware was detected
tantial evidence such as this indicates that attackers are actively
new malware creations against popular anti-virus programs to ensure
y undetected

ddition, malicious actors exploit the distributed and global nature of
rnet as well as the complications of law and jurisdiction bound by
al physical boundaries to diminish the risks of being identified and
ted For example, a large portion of data trapped by attackers using
ers is transmitted internationally to countries where laws against
me are nascent, non-existent or not easily enforceable Although
s across the globe have recognised the seriousness of cybercrime
y have taken legislative action to help reprimand criminals, not all
al frameworks that support the prosecution of cyber criminals [13] The

enforcement agencies throughout the world have made efforts to te cyber criminals. For example, the Computer Crime and ual Property Section of the US Department of Justice has reported ecution of 118 computer crime cases from 1998 – 2006 [14] Although tatistics on arrests are hard to determine, one company estimated de arrests at 100 in 2004, several hundred in 2005 and then 100 2006 (Greene, 2007). While these cases did not necessarily involve , they help illustrate the activities of the law enforcement nity. It is important to note that the individuals prosecuted are responsible for multiple attacks. These figures are low considering valence of online incidents and crime. They highlight the complex es faced by law enforcement in investigating cybercrime.

hermore, the volatile nature of electronic evidence and the frequent logged information can often mean that evidence is destroyed by the w enforcement officers can get the necessary warrants to recover ent. The bureaucracy of law enforcement provides good checks and s, but is often too slow to cope with the speed of electronic crime. nally, incident responders often do not understand the needs of law ment and accidently destroy electronic evidence.

ay, the benefits of malware seem to be greater for attackers than the undertaking the criminal activity. Cyberspace offers criminals a mber of potential targets and ways to derive income from online. It also provides an abundant supply of computing resources that can essed to facilitate this criminal activity. Both the malware and mised information systems being used to launch the attacks have a t, are readily available and frequently updated. High speed Internet ions and increased bandwidth allow for the mass compromise of tion systems that renew and expand the self sustaining attack. By contrast, communities engaged in fighting malware face us challenges that they cannot always address effectively.

Notes

iis could be the case for any Internet connection, broadband or herwise

or the purposes of this measurement, Symantec defines "targeted attack" an IP address that attacks at least three Symantec sensors in a given ctor while excluding the other sectors during that reporting period See ymantec (2007), p 85

2004 report from the U S Joint Council on Information Age Crime owed that 36% or less of organisations polled reported computer-lated crimes to law enforcement See US Joint Council on Information ge Crime (2004), p 8

this case, direct damages refer to labour costs to analyse, repair and eanse infected systems, loss of user productivity, loss of revenue due to ss or degraded performance of system, and other costs directly incurred the result of a malware attack Direct damages do not include eventive costs of antivirus hardware or software, ongoing personnel sts for IT security staff, secondary costs of subsequent attacks enabled the original malware attack, insurance costs, damage to the ganisation's brand, or loss of market value [Note Issues include nited sample sizes, limited responses, inability to accurately estimate e costs of a malware incident, the difficulty in detecting malware cidents, and so on In all cases, references should be to estimated sses]

ich losses were not measured in the survey

e Chapter 2 for a more detailed discussion of how malware may subvert ese security technologies and counter-measures

ustralian Government, Office of the Privacy Commissioner (2004), onsumer Reports WebWatch (2005), Gartner (2005), RSA Security

JS v James Brewer", United States District Court Northern District of inois Eastern Division (2007)

recent OECD report, *The Development of Policies to Protect the ritical Information Infrastructure*, highlights this point See OECD 008c).

S.-Canada Power System Outage Task Force (2003), p. 131

formation provided to the OECD by CERT.br, the national CSIRT for razil

ne website provides a survey of cybercrime legislation that documented countries with some existing cybercrime law See *tp://www.cybercrimelaw.net/index.html*.

nited States Department of Justice Computer Crime & Intellectual roperty Section (2007)

Part II. The Economics of Malware

hel J G van Eeten[1] and Johannes M Bauer[2]
ntributions from Mark de Bruijne, Tithi Chattopadhyay, Wolter , John Groenewegen, and Yuehua Wu

ualware is a product of criminal behaviour, its ultimate magnitude pact are influenced by the decisions and behaviour of legitimate participants, such as Internet Service Providers (ISPs), software e-commerce companies, hardware manufacturers, domain name rs and, last but not least, end users. Part II of this book presents ive empirical research into the incentives that drive the security s of Internet market participants. The results of this research a number of market-based incentive mechanisms that contribute to d security. But there are also instances in which decentralised may lead to sub-optimal outcomes - i.e. where the consequences of ate security measures are "externalised", or borne by others in the or society at large.

of this book is an edited version of an original OECD working paper ed "The Economics of Malware", the content of which is available //dx.doi.org/10.1787/241440230621.

lty of Technology, Policy and Management, Delft University of

pter 4. Cybersecurity and Economic Incentives

past five years have witnessed the emergence of comprehensive
to improve the security of information systems and networks. A
urvey by the OECD (2005a) demonstrates that governments have
ed national policy frameworks, as well as partnerships with the
sector and civil society, to combat cybercrime. Measures include
er Security Incident Response Teams (CSIRTs), raising awareness,
tion sharing and education

improving cybersecurity is not a straightforward problem.
standing rapidly growing investments in security measures, it has
clear that cybersecurity is a technological arms race that, for the
ate future, no one can win. Take spam, for instance. Several years
called open e-mail relays were a major source of spam. ISPs and
tors developed measures, such as blacklisting, to collectively combat
ays. By the time adoption of these measures reached a critical mass,
rs had already shifted their tactics. As a result, the significant
n in the number of open relays had hardly any impact on the amount
. The list of such examples goes on and on.

le many would agree that cybersecurity needs to be strengthened,
ctiveness of many security measures is uncertain and contested.
more, security measures may also impede innovation and
vity. Those involved in improving cybersecurity sometimes tend to
k that the reason why the Internet is so susceptible to security threats
ly its openness – is also the reason why it has enabled an
linary wave of innovation and productivity growth.

ie Internet world, the benefits of productivity growth often outweigh
s of innovation – as in the case of online credit card transactions.
e start of moving their business online, credit card companies have
d with rising fraud. However, this has not stopped them from

and Carter, 2005) Rather than implementing far-reaching security s that would restrict the ease of use of their systems, credit card ies have adopted strategies to fight instances of fraud, up to the point he costs of further reductions in fraud start to exceed the benefits, avoided

this means that total security is neither achievable nor desirable In e, actors need to make their own tradeoffs regarding what kind of measures they deem appropriate and rational, given their business Clearly, business models vary widely for actors in the different of the complex ecosystem surrounding information systems and s – from ISPs at different tiers to software providers of varying ions, to online merchants to public service organisations and to end ll of these actors experience malware differently, as well as the costs efits associated with alternative courses of action In other words, stances of what could be conceived as security failures are in fact ome of rational economic decisions, reflecting the costs and benefits d by the actors during their decision-making timeframe.

at is needed, then, is a better understanding of these costs and from the perspective of individual actors and of society at large f this report sets out to identify the incentives under which a variety net market participants operate, and to determine whether these es adequately reflect the costs and benefits of security for society – ther these incentives generate externalities To address these issues, ings are presented of a recent research project on incentives that elp lay the groundwork for future policymaking.

cus on incentive structures

earch in the field of cybersecurity is undergoing a major paradigm ore and more researchers are adopting economic approaches to study curity, shifting emphasis away from technological causes and s. Most of this innovative research has yet to find its way into the f policy makers, let alone into the policies themselves While reports OECD survey on the culture of security (OECD, 2005a) generally e that cybersecurity is more than a technological issue, the proposed s are still mostly oriented in that direction developing technological es and efforts to stimulate their adoption The technological

x 4.1 OECD Guidelines and the Economics of Cybersecurity

002, the OECD released the *Guidelines for the Security of Information s and Networks* (OECD, 2002a). A set of nine non-binding guidelines aim note "a culture of security" – that is, "a focus on security in the ıment of information systems and networks, and the adoption of new ways ıing and behaving when using and interacting within information systems 'works" – among "all participants in the new information society" (see The guidelines reflect the shared understanding of OECD member es as well as a variety of business and consumer organisations

Guidelines for the Security of Information Systems and Networks

wareness
articipants should be aware of the need for security of information systems nd networks and what they can do to enhance security

esponsibility
ll participants are responsible for the security of information systems and etworks

esponse
articipants should act in a timely and co-operative manner to prevent, etect and respond to security incidents

thics
articipants should respect the legitimate interests of others

emocracy
he security of information systems and networks should be compatible ith essential values of a democratic society

isk assessment
articipants should conduct risk assessments

ecurity design and implementation
articipants should incorporate security as an essential element of formation systems and networks

ecurity management
articipants should adopt a comprehensive approach to security anagement

eassessment
articipants should review and reassess the security of information systems nd networks, and make appropriate modifications to security policies, ractices, measures and procedures

"culture of security" that the guidelines aim to promote will be influenced

x 4.1 OECD Guidelines and the Economics of Cybersecurity (continued)

pter 5 provides a more detailed discussion of why this is the case. For now, ces to mention a few examples. Take firms' investment in security es. Research has demonstrated that a focus on security may mean actively ating in information sharing with other firms. Under certain conditions, ually leads to decreased investment levels. Also, a firm taking protective es may create positive externalities for others – that is, benefits for others not reflected in the decision by that firm – which may reduce their ents to a level that is below the social optimum.

ther example is the manufacturing of software. According to the *OECD nes* (OECD, 2002b), "Suppliers of services and products should bring to secure services and products." Even if it was clear what the term "secure e" means, many software markets do not reward such behaviour. Rather, ward first movers – that is, those companies that are first in bringing a new to market. This means it is more important to get to the market early, han first investing in better security. A final example relates to end-users. *idelines* argue that end users are responsible for their own system. In the malware, however, this responsibility may lead to security tradeoffs that onal for the end users, but have negative effects on others. More and more e actively seeks to reduce its impact on the infected host, so as not to be d or removed, using the infected host to attack other systems instead of the elf.

hort: the development of a "culture of security" is very sensitive to ic incentive structures. Whether such a culture will actually improve security performance requires a better understanding of the incentives which actors operate as well as policies that address those situations in ncentives produce outcomes that are not socially optimal. The research presented in this Part II of the malware report aims to contribute to this king.

withstanding the necessity of these initiatives, they typically k the economic factors affecting cybersecurity – *i.e.* the underlying ic incentive structure. As Anderson and Moore (2006, p. 610) have "over the past 6 years, people have realised that security failure is at least as often by bad incentives as by bad design." Many of the s of information security can be explained more clearly and ngly using the language of microeconomics: network effects, rties, asymmetric information, moral hazard, adverse selection,

he second part of the 1990s, when the scale of virus distribution was ncreasing and countless end users (home, corporate, governmental) ected, many ISPs argued that virus protection was the responsibility nd users themselves. The computer was their property, after all. ISPs argued that they could not scan the traffic coming through their e-rvers, because that would invade the privacy of the end user. Mail es were considered the property of the end users.

ut five years ago, this started to change, partly due to the growth of nd and always-on connections. The distribution of viruses and had increased exponentially and now the infrastructure of the ISPs ves was succumbing to the load, requiring potentially significant ent in network expansion. Facing these potential costs, ISPs y shifted their position. Within a few years, the majority of them to scan incoming e-mail traffic, deleting traffic identified as nt, since this had become a lower-cost solution than infrastructure on. *De facto*, ISPs re-interpreted the various property rights ed with e-mail – *e.g.* regarding ownership of the message. Their l policies have made e-mail based viruses dramatically less effective ack strategy.

ic perspective

economic perspective on cybersecurity – and malware in particular – a potentially fruitful starting point for future policymaking. That's it leads to a focus on market participants' (1) incentive structures market externalities, or the consequences of inadequate security s that are borne by other market participants or society in general.

his chapter and those following, the economic perspective on and cybersecurity are examined, building on the innovative efforts of the past six years (for a brief overview of the existing e, see Anderson and Moore, 2007; Anderson *et al*, 2008). It is a first his direction, and given the complexity of the problem, more work oubtedly be needed.

promising approach is to complement the existing research with ualitative field work. Field research is important because there is information in the public domain on how Internet market

Box 4.2 The problem with prevailing research methods

ar, most of the Internet-related economics research has been based on the s of neo-classical and new institutional economics. While powerful, these s are based on rather stringent assumptions about how actors behave – their rationality, their security tradeoffs and the kind of information they and how they interact with their institutional environment.

e key limitations of studies founded on these methodological assumptions

- they provide limited insight into how actors actually perceive the cost, benefits and incentives they face,
- they have difficulty taking into account dynamic and learning effects, such as how a loss of reputation changes the incentives an actor experiences, and
- they often treat issues of institutional design as rather trivial. That is to say, the literature assumes that its models indicate what market design is optimal, that this design can be brought into existence at will, and that actors will behave according to the model's assumptions.

e past decade of economic reforms – including privatisation, liberalisation egulation – have taught us anything, it is that designing markets is highly ated and sensitive to the specific context in which the market is to n. It cannot be based on formal theoretical models alone. Institutional requires an in-depth empirical understanding of current institutional es and their effects on outcomes. Even with such an understanding, it may possible to fully control the setup and working of a market as they are in nerging from the interaction of multiple actors. However, it should be e to nudge the system in the desired direction.

II presents efforts to: (1) collect evidence on the security tradeoffs Internet market participants, (2) how those participants perceive the es under which they operate; (3) which economic decisions these es support, and (4) the externalities that arise from these incentive es. The objective of Part II is to contribute to the debate on the ics of malware from an empirical and analytical perspective. It is not d to explore and develop detailed policy recommendations.

pter 5 reports the findings of the field work. Based on 41 interviews 7 representatives of Internet market participants, as well as

pter 6 aggregates the research findings and discusses the ities that emerge as market participants make incentive-driven decisions. In some cases, externalities are borne by market ants able to influence the security tradeoffs of those generating the ities bringing the net market impact closer to the optimum. In other ne externalities are simply borne by market participants or by society . Part II concludes with a summary of the efficiency and ional effects of externalities and an overall assessment of the costs are

annex at the end of Chapter 5 contains a list of the survey ants. Annex B at the end of this report describes the survey in detail.

Chapter 5. Survey of Market Participants: What Drives Their Security Decisions?

icipants in the Internet ecosystem are confronted with malware in t ways, their responses are motivated by the specific incentives hich they operate. To better understand these incentives and their a qualitative field research project was designed. In the course of e research team conducted 41 interviews with 57 respondents from a oss-section of organisations. (For more information on the research nd the interviewees, please see the list at the end of this chapter and 3.)

ow, we discuss the findings on the security-related incentives of five nternet segments. Internet Service Providers (ISPs), e-commerce ies (with a focus on online financial services), software vendors, registrars, and end users. Interviews were also conducted with tatives of organisations governing security issues (such as CERTs, ry agencies), representatives from security service providers, and searchers.

vice providers

le the term ISP is used to cover a variety of businesses, typically ovide individuals and organisations with access to the Internet. Many fer related services to their customers, which is why the term es also refers to hosting providers and content providers. For the s of this study, we focus our analysis primarily on ISPs that provide access.

role of ISPs in improving Internet security has been the focus of ecent debates. That's because it has proven extremely difficult to

ably lower – *e.g.* Trend Micro published a figure of 7% (Higgins
Nevertheless, even these lower estimates imply tens of millions of
nised machines. Given the enduring problems around end-user
and its effects on the wider network, it seems inevitable that
n would shift to other players in the ecosystem.

at incentives do ISPs have to reduce the problem of malware? One
very few, if any. Recently, the UK House of Lords Science and
ogy Committee published a report which states: "At the moment,
n ISPs could easily disconnect infected machines from their
s, there is no incentive for them to do so. Indeed, there is a
tive, since customers, once disconnected, are likely to call help-lines
e up the time of call-centre staff, imposing additional costs on the
louse of Lords 2007a, p. 30)

s may unwittingly reinforce the impression that they have few, if
entives to improve the security of their services. During the inquiry
to the House of Lords report, ISPs argued that the current approach
egulation should not be changed. The resistance of most ISPs to
d government involvement led the committee to conclude that the
ere simply maintaining the status quo, rather than reducing the
. The latter, however, does not follow from the former. The
ce to government involvement does not mean that ISPs are not
ng their efforts to fight malware. In fact, the committee itself also
idence from an ISP who in fact disconnects customers whose
es had been infected and then helps them back online. A survey from
s European Network and Information Security Agency found that
ISPs report that they quarantine infected machines (ENISA, 2006).
ure does not include any indication of the scale at which ISPs are
ning infected machines – a point to which we return in a moment.
dence does, however, clearly question the earlier statement by the
ee – and others – that ISPs have no incentives to disconnect infected
s. Either the statement is wrong, or ISPs are assumed to behave
ally. Our evidence suggests the former.

ISPs we interviewed described substantial efforts in the fight against
, even though they are operating in highly competitive markets and
no governmental regulation requiring them to do so. All of them
king measures that were unheard of only a few years ago. Most of
rviewees dated this change to around 2003, when it became obvious

entives

customer support and abuse management

understanding of these incentives could start with this statement by a officer of a smaller ISP: "The main [security-related] cost for ISPs mer calls." The same view was expressed with minor variations by other interviewees. A medium-sized ISP told us that an incoming their customer centre costs them EUR 8 on average, while an g call – for example, to contact the customer regarding an infected – costs them EUR 16. The costs for e-mail were similar. When we ed these numbers during subsequent interviews with other ISPs, firmed that their costs were in the same range.

incentive here is that security incidents generate customer calls, ickly driving up the costs of customer care. The ISPs may not be responsible for the customers' machines; in reality many customers ir ISP whenever there is a problem with their Internet access. ess of the subsequent response of the ISP, these calls increase their n interviewee at a large ISP told us that their customer support desk ubstantial cost for the company, and that the number of calls was p by infections of their customers' machines. He further added that ll of their outgoing security-related calls had to do with malware.

course, many forms of malware do not manifest themselves y to customers. Nevertheless, as security problems rarely come ax security generally tends to increase customers calls. Furthermore, customers have not noticed anything wrong, their compromised s may generate abuse notifications to their ISP from other ISPs who incoming spam or malware from the customer's IP address. Similar mer contact, dealing with abuse notifications drives up costs because es trained staff. Tolerating more abuse on the network raises the of notifications that have to be investigated, responded to and acted Acting may mean filtering the customer's connection or even ing it altogether, until the problem gets resolved. All the ISPs we wed have procedures in place for handling abuse notifications and do ilter and suspend connections, though with varying frequency. All of so mentioned a small number of cases where extreme forms of abuse e termination of the contract.

form. Many of these notifications are automated. Several ISPs
l using the so-called AOL Feedback Loop, which sends notifications
e-mails that are reported as spam by AOL recipients back to the
trator of the originating IP address.

with customer complaints, not all malware infections will result in
otifications. One ISP reported internal research into the degree to
otifications adequately represented the size of the security problems
r networks. They found that only a small percentage of the
nised machines they saw on their network showed up in the
ions. Still, ISPs notifying each other of security problems is an
nt mechanism. In fact, in some cases, they are critical. In some
n countries, ISPs have interpreted the stringent privacy regulations
that substantially limit their ability to monitor their own network. In
ses, they rely heavily on notifications coming in from other ISPs,
hen allow them to initiate their own investigation. For the ISPs we
wed, customer contact and abuse notifications are a strong incentive
t in security both at the network level, as well as at the level of the
r. One medium-sized ISP estimated they were spending 1-2 % of
verall revenue on security-related customer support and abuse
ment. This also helps to understand why more and more ISPs are
"free" security software or "free" filtering of e-mail – that is, the
f these services are included in the subscription rate. One ISP
d how about four years ago they started offering virus filters for e-
n paid service, but soon thereafter decided to provide them for 'free':
ix months, all ISPs [offered these paid security services], so it was
er a unique selling point. Plus, we could not get more than 10 % of
omers to buy the service. We did not actually do the math, but we
that by offering it to all our customers within the current rate, we
e better off. We already paid the AV license. If people have the
o pay for it or not to pay for it, they do not."

re is another way of responding to these incentives, however. Don't
to abuse notifications and avoid customer contact altogether. A
ISPs is doing exactly this. What is stopping other ISPs, including
we interviewed, from doing the same? Here, we came across two
ted relevant incentives: blacklisting and brand damage.

f blacklisting

of blacklists available and ISPs may use them in different
ations.

ording to many interviewees, most ISPs use blacklists nowadays.
the lists are free and run by volunteers, though their operations may
ed through external sources. Each DNSBL has its own criteria for
g an IP address in the list and its own procedure for getting an
off the list. Spamhaus, an international non-profit organisation
through sponsors and donations, maintains several famous blacklists
h they prefer the term block lists – which they claim are used to
over 600 million inboxes. One of their lists contains the addresses of
ources, including spammers, spam gangs, spam operations and spam
services", another list focuses on botnets, which run as open

hould be noted at this point that blacklisting, while potentially
l, has drawn its own criticisms – regarding, among other things,
sm of blacklist operators, listing false positives, the collateral
that may come with blacklisting certain IP addresses or ranges, and
ncial motives of some list operators. Furthermore, blacklists have
from legal threats; in some cases, spammers on occasion were
ul in obtaining court verdicts against being blacklisted (*e.g.*
an, 2006; Heidrich, 2007). Within this report we focus on how
ting works as an incentive for ISPs.

klisting provides an incentive to invest in security because it ties in
incentives mentioned earlier. One interviewee at a medium-sized
us about a security incident where 419 spammers set up over 1,000
accounts within their domain and then started pumping out spam.
t the ISP's outbound mail servers blacklisted, which resulted in 30
s to their customer centre by customers who noticed their e-mail was
r being delivered. That number does not include the incoming abuse
ions, of which there were "even more". After this incident, the
y changed the procedure through which new customers can set up e-
ounts; they invested millions in equipment to monitor their network;
y started blocking port 25. "It took us years to get a procedure
d to be able to block port 25. It costs nothing. But the business units
want us to be able to shut it down, because of their clients. They now
nd that it is in the interest of their clients, to avoid blacklisting."

the customer does not resolve the problem, the connection is
ed. When asked how they got the business side of the company to
this policy, he answered:

ey hated it at first. But at the end of the day, the media fallout by
ut off by AOL and MSN is too big. The big ISPs, they use very
ve [DNSBL] listings. They take out whole IP ranges. We used to be
and entire ranges of our IP addresses were blacklisted."

re are various levels of blacklisting used to incite a response from an
the lower end, we find blacklisting of individual IP addresses, *i.e.* an
ual customer. This has "exactly zero impact on the ISP," said a
expert. Only when they start to accumulate, might they get the ISP's
n. The expert explained that ISPs mostly ignore listed individual IP
es, because of the costs of dealing with them – *e.g.* customer support
ecause the IP addresses gets taken off of the blacklist as spammers or
s move on to other infected machines. After a few months, the level
e infected machines on the ISP's network might be equally high, but
fferent set of individual IP addresses that are now blacklisted.

cklisting IP ranges and the blacklisting outbound mail servers are a
owerful incentive. These typically do get the ISPs attention and lead
dial action on their end, although it varies whether or not the ISP
vigilant. The most extreme form is blacklisting an entire network,
P addresses of an ISP. This is only used against semi-legitimate ISPs
ot act against spam and known spam-havens.

f brand damage and reputation effects

"media fallout" mentioned previously by an interviewee indicates a
eneral concern with brand damage that was mentioned by many
wees as an incentive to invest in security. With few exceptions, these
nt to present themselves as responsible businesses (Arbor Networks,
roviding safe services for their customers.

elated incentive is the reputational benefits of offering security
. The increasing attention on Internet security – or rather, to the lack
– is creating demand for such services. One interviewee said: "The
sk us for 'clean pipes.' We do not know what that means exactly, but
us anyway. We're looking into what we can do for them." The past
ve witnessed the emergence of managed security service providers,

f security may be a significant factor. For the consumer market, terviewees argued that customers care about price first and foremost s, Internet access is marketed primarily on price. Furthermore, even do care about security, most customers will find it very difficult to he security performance of one ISP relative to its competitors. eless, the more significant finding here is that whether ISPs really ut bad publicity or not, being blacklisted has direct effects on their g costs, as well as their quality of service. The latter may in fact stomers away. As one industry insider described it: "A high cost to investigate each complaint rigorously. A different kind of high on is to do nothing."

f infrastructure expansion

ncentive that was more difficult to gauge, is the effect of malware capital expenditures of the ISP – that is, the need to expand cture and equipment as more spam or malware comes through the . A recent survey found that botnet-based denial of service attacks ving faster in size than the ISPs are expanding their network – which ing the ISPs (Arbor Networks, 2007).

restingly, infrastructure expenditures – apart from the costs of equipment – were hardly identified during interviews as malware-costs, a point to which we return shortly. As was mentioned earlier, wees pointed to customer contact as the highest security-related cost. sked about infrastructure, a Chief Technology Officer answered: twork is not affected. We have overcapacity to deal with DDoS. So ot the problem."

another ISP, the Chief Information Security Officer told us: "We to have overcapacity of the network, so the growth in spam did not us to expand the capacity." To which one of his colleagues added: number of servers has increased, though." Others have argued that me of malware and spam-related traffic pales compared to the traffic peer-to-peer networks and video streaming sites such as e.com. We should add, however, that the presence of overcapacity flect the fact that we only interviewed ISPs in selected OECD s. It may be different in other regions.

en we presented these findings to an expert in the economics of

-related customer support. To them the infrastructure cost "is just a their accountant writes on a check every month."

vever, infrastructure is the main overall cost for any ISP, so any f malware on capital expenditures could potentially outstrip other tures. These costs do not gradually increase with the amount of and spam, but rather as a step function when capacity runs out. It is ficult to relate these expenditures back to specific traffic patterns of d malware infections. Only higher up in the organisation are people ition to compare the relevant numbers, although at that level the y security expertise and data is often missing. The interviewee hat there are really three groups of people who all see a part of the , without being able to cross-connect it: "One group is dealing with , one group is dealing with the capital expenditures and engineering t and another group is dealing with handling the money." In terms itives, however, this lack of awareness implies that infrastructure not a strong driver of the attempts of ISPs to reduce the impact of .

s of maintaining reciprocity

incentive that was mentioned by all interviewees is related to the l networks of trusted security personnel across ISPs, CSIRTS and organisations – which we mentioned earlier. When describing how ganisation responded to security incidents, interviewees would refer onal contacts within this trust network that enabled them, for , to get another ISP to quickly act on a case of abuse. There is not ormal network, but rather several overlapping ones. An ISP may h a contact at a national CERT in another country so as to get in ith the relevant person at an ISP in that country. These contacts are al. They are also contacted about abuse in their own network and are d to act on that information. The incentive is that to maintain ity, an ISP has to treat abuse complaints seriously, which is costly. re abuse takes place on its network, the more other contacts in the will ask for intervention.

ntaining reciprocity not only establishes the informal network as a resource, it also reduces the likelihood of being hit with blacklisting countermeasures. As one interviewee explained, "when we get in ith service providers, we're saying, get this guy off the network or

e leeway to deal with security issues before significant blacklisting One ISP security officer told us that these informal contacts imply ings. Less staff time is needed to deal with the fallout of a security – *e.g.* going through time-consuming procedures to get off ts – and to deal with customer support

ncentives

f security measures

far we have discussed incentives that reinforce the benefits of for ISPs with regard to malware. The incentive structure is mixed, r, and includes disincentives as well. An obvious disincentive is the additional security measures. Typically, the trade-off is between the osts of additional measures, which are visible in the short term, he costs generated by increasing security problems, such as customer and abuse management. A security expert at a large ISP told us that agement it is difficult to estimate the amount of money the company e with a technical solution which is supposed to reduce the costs of e desk or call centre. Another interviewee added that a complicating as that managers had encountered over-promising security providers d them 'magic boxes' that were supposed to solve everything.

should mention, however, that the ISP's decisions often were not by formal economic assessments or detailed analysis of their own ictures. As one insider phrased it, "ISPs very much drive by the seat pants. Except for a very few of the largest ones, they are not actually ng the figures." When we asked how certain investments or s were approved, the "business case" that supported them was y rather commonsensical in nature, including rough estimates of osts and benefits, with the indirect ones not monetised or otherwise d in any amount of detail.

interviewee told us that when considering security investments, ook at the cost of *not* doing it" for which they produce rough s. Another ISP explained to us how they decided to set up a so- 'walled garden experience' for infected users. Rather than ecting these users completely, the 'walled garden' provided them cess to security tools and Windows Update. A security officer

isks and constraints

ther disincentive is related to legal constraints. During the ws, the European ISPs had different answers to the question on how anoeuvring space the 'mere conduit' provision of the EU E- rce Directive allowed them. Monitoring their network more closely rity reasons could potentially lead to liability issues, some of the wees felt. In some EU countries, interviewees reported that privacy ons that potentially treat IP addresses as private data had led their partments to set boundaries which affected the ability of the security track malicious activity on their network – for example with regard ng individual IP addresses.

interviewee reported that security staff sometimes were not allowed nformation on malicious activity detected on the network. When bout the limits of the 'mere conduit' provision, one security officer ed that they never encountered these limits, because the privacy ons were much more constraining. Rather than monitoring their own , this particular ISP could act on incoming abuse notifications for IP addresses and it relied heavily on this procedure. In a sense, the s monitoring its own network through the incoming notifications ner ISPs, CSIRTs and the like.

where there have been reports over liability issues around measures, such as discarding the command and control traffic of a or diverting it to where the botnet's behaviour can be studied more (Higgins, 2007a). According to a security researcher "it involves g with a customer or peer's Internet address space. Obviously, in this area could be considerable." A security manager at a n ISP said "infiltrating is very risky and getting legal support for tters, very difficult."

he legal experts argued that these legal risks are non-existent, that based on an incorrect understanding of current legislation – *e.g.* that data protection legislation does not at all conflict with network ng and other security measures. While that might be true, the reality he legal departments of some ISPs apparently interpret the situation – mistakenly – as rather ambiguous. These ISPs tend to be rather risk n dealing with this ambiguity. The transaction costs of clarifying sues are, *ceteris paribus*, an obstacle to higher security.

e business side of their company initially opposed the security
to block port 25. They did not want to inconvenience their
rs. Anything that might turn people away is a problem, because the
cquisition of new customers is high. The burden of proof fell on the
staff to convince management that the proposed measures were
ng the brand. Other ISPs also mentioned going to great lengths to
osing customers while managing abuse. That might limit the
eness of their response to security incidents.

ISPs

ue of the security-enhancing incentives discussed above work as
tives under different business models than those of the ISPs we
wed. When dealing with abuse complaints becomes too costly, one
er reduce the amount of abuse on the network or one can reduce
ment of abuse – i.e. become less responsive to the complaints
ves. The same holds for customer support. In fact, such a lack of
could be part of the business model. It may, for example, allow an
be cheaper than its competitors. One ISP indicated that a certain
of its customers was actually "mini ISPs" which predominantly
hosting services. The mini ISPs' retail prices were significantly
han those of the upstream ISP from which they bought access,
they provided very limited support functions. Some of these mini
uld not patch their servers properly, thus becoming an easy target
ware. They were not very responsive to abuse complaints either. Our
wee, being an upstream access provider, would then be contacted by
Ps to take action against the mini ISP.

ther business model is sometimes referred to as "rogue ISP" or ISPs
, in the words of one interviewee, "decidedly grey". These attract
rs precisely because of their lax security policies. While these ISPs
re disincentives for improving security than the ones interviewed,
not fully immune to some of the security-enhancing incentives we
d earlier, most notably blacklisting. As one interviewee explained:
are some ISPs in our country that are decidedly grey. They will take
and take no action against abuse. People will go there and then they
ve again, because they are unreachable [because of blacklisting]."
ogue business models are eventually affected by blacklisting.
ly, a Ukrainian ISP started answering our abuse reports," the

a provider who is in fact security conscious and sensitive to the es discussed earlier, such as maintaining reciprocity and ting. In the example of the mini ISPs, their upstream provider forces deal with abuse complaints, because it reflects badly on the n provider if they do not. Beyond blacklisting, there is also de- – that is, an ISP may disconnect from a misbehaving ISP at an exchange point. For the ISPs we interviewed, this is not an nt incentive, because de-peering for security reasons is typically only ed against rogue ISPs, not among regular ISPs. De-peering forces the ected ISP to buy transit service for its traffic, which implies much perating costs.

ry of ISP incentives

balance between incentives and disincentives will vary depending SP. On the whole, recent years have witnessed increased efforts by dealing with malware, even in the absence of regulation or other of public oversight. The incentive mechanisms we discussed en the ISP's own interest to internalise at least some security ities originating from their customers, as well as from other ISPs. In he current incentive structure seems to reward better security ance for legitimate market players – though it is sensible to keep in at in many countries price competition is intense, which is a tive with regards to security, other things being equal.

centives to confront malware	**Disincentives**
Lower customer support costs Less blacklisting Maintaining reciprocity Maintaining reputation and amming brand damage	• Costs of security • Legal restraints • Costs of customer acquisition

ey considerations for ISPs

ation

ically generated a list of 2 500 IP addresses a day of customers who
me form of security problem. When these cases hit a certain
d, they would be automatically quarantined to only have access to
s Updates and a range of security services.

le the technologies to automate the process of quarantining would
scale up the ISPs response, it also brings into focus a critical
ck: the costs of customer support would become prohibitive if all
machines were to be quarantined. A security officer at a large ISP
d that the number of customers that would be affected at any time
e in the tens of thousands. While this number might go down over
network security improves, it was obvious that the business side
ot accept the cost impacts of such a measure.

ically, the number of machines that are isolated on a daily basis is
y modest – tens or, for large ISPs, perhaps hundreds of machines. At
el, the effort is effective in that it reduces the ISP's problems with
nd blacklisting. But compared to estimates of the total number of
is on each network, these efforts look rather pale. When asked to
he ratio between the actual number of infected machines on their
and the number of machines for which they receive abuse
ions, most interviewees estimate that the ratio is quite low. Only a
ercentage of these machines would show up in abuse notifications
dealt with. One interviewee called this "the two percent rule". A
expert was highly critical of the effectiveness of the efforts by ISPs:
they are contacting more than 10 % of their customer base on a
basis, they are effectively taking no action".

it of ISP incentives

elated issue is that the incentives of ISPs do not reflect the whole
f current malware threats. ISPs are predominantly sensitive to
that manifests itself in ways that make their customers call in, leads
notifications or that causes problems with blacklisting. That means
oxies and DDoS (denial of service) attacks attract attention and raise
hile spyware, for example, does not. "People get infected and it is
ficult to track them. Spam and DDoS is noticeable at the network
ut spyware stays on the computer, quietly collecting data." Others
gued that many ISPs are failing to prohibit the forging or spoofing of
esses by hosts as well as failing to filter outgoing traffic from IP

machine. Even then, the situation is often anything but orward. "The issue is, how do you help the people who are infected, e current state of the security products in the market place? We see ic, we know there's something wrong, but how do you find what it is current products? It's very hard. About 85-90% of the malware is gnised by AV products, because a small change is enough to dodge ature."

g with rogue ISPs

other important caveat is that there are classes of ISPs for which the es to improve security are too weak, or which even have strong tives to improve it, as discussed above. The ISPs we interviewed existence of such ISPs as a fact. Because it is possible for rogue stay outside the reach of legislation and law enforcement, they are be present for the foreseeable future. The ISPs we interviewed have to live with the presence of the rogue and semi-legitimate ISPs ave found that they are able to operate quite effectively in this ment through a combination of tactics, including those mentioned such as informal contacts that address upstream providers and ing.

he mind of ISPs, no matter what policies, governance structures or es are put in place there will always be some providers, outside or heir own jurisdiction, who will be a source of malware and other f abuse. Once this is accepted, then it is also accepted that an ISP has defenses and develop procedures for dealing with attacks. "You will have to accept a certain level of noise, that is, of evil. You try to below a certain threshold of irritation" said a security officer. This is the reasons why many ISPs are not impressed by proposals to some set of baseline or best security practices for ISPs. One such was under development by the Dutch electronic communications r OPTA but it was shelved for the time being after significant k regarding the legal basis for such regulations. The recent report of House of Lords Science and Technology Committee (2007a, p. 31) vocated making "good practice... the industry norm[, by means of on if necessary.]"

fact that ISPs can work within the insecure status quo does not at their responses are static or complacent. The status quo actually

companies

multitude of companies that buy and sell products or services over rnet operate on a wide variety of business models, each with t incentive structures for security. We have chosen to focus on financial services, since they have been an important target of attacks, arguably more than any other sector (Counterpane & eLabs, 2006). This includes brick-and-mortar banks that are offering their service portfolio online, credit card companies, as well as nly financial service providers, such as PayPal. The sector has been ted with a wide range of threats ranging from botnet-assisted spam runs and phishing websites, to keyloggers and Trojans that man-in-the-middle attacks during secure banking sessions.

ve: increased online transaction volume

ey incentive for all these companies: a growing volume of online ions. Credit card companies and online financial service providers y charge a fee per transaction, either a flat amount or a percentage of saction. The situation is somewhat different for brick-and-mortar For many of their services, they do not make any money from the ion itself. Their incentive to pursue online banking is the able cost savings that it enables. Two of the interviewees in the l sector estimated that online transactions were in the order of 100 heaper than processing those transactions offline, through their offices, mail or phone. Given the enormous volume of financial ions, costs savings of that magnitude translate into a very powerful e to move online as much these services as possible.

v does this incentive affect security decisions? To answer that , we need to understand how transaction volume interacts with other incentives: the benefits of trust in the online services, the of usability, the cost of security measures, and the cost of fraud.

ve: consumer trust

hin the sector, it is assumed that consumer trust in the security of ervices is a necessary condition for their uptake. This rewards g in security. Beyond this generic consensus, however, views

eral consumer surveys suggest that security problems turn people om e-commerce and online banking, in particular. The 2006 UK Get line survey reported that the fear of falling victim to Internet crime 4% of respondents from Internet banking and has put off 17% from use all together (GetSafeOnline, 2006). It is difficult to interpret the g of these findings when compared to other data. For example, most l service providers still report significant growth rates in the n of their online services (PayPal,2007). These two seemingly ctory pieces of evidence point out that the role and impact of trust is adequately understood. An industry study of trust in e-commerce e *et al*, 2006) argued that "[w]hile an initial hypothesis may be that do not engage with online services because they do not trust them, lings have shown that trust is not as significant a measure as first

at is more important to understand is that people are willing to take line, as long as they are informed, and it is clear how consequences addressed. People use specific services not because they trust them, ause they in some way provide a benefit to the individual and they at if something goes wrong, restitution will be made." This suggests important factor driving the use of online financial services is not the trust in the security of these services, but the more specific ion that a customer will be compensated in case of fraud. In other rom a customer's perspective, it seems more important that financial providers assume liability for online fraud than that they achieve a evel of – perceived – security.

de-offs

and usability vs. security

uming that increased security increases consumer trust and, in turn, s the uptake of online services, this effect would still need to be l against the effects of increased security measures on the usability service. One of our interviewees at a bank with an international e explained that the national branches of his company positioned ves differently with regard to this trade-off. While in some countries, or authentication was readily accepted, in other countries the bank its customers were less open to such security-enhancing technology.

g usability and security, these companies try to maximise the of online financial transactions, while keeping the level of fraud at able levels.

online volume vs. losses due to fraud

ther important incentive for security is the fraud losses that any the increasing volume of online transactions. In the United banks are liable for direct fraud losses under the Electronic Funds Act of 1978 – also known as "Regulation E". Under this regime, rs are compensated for such losses, unless the bank can prove that omer's claims are false. In many other jurisdictions, the banks are speaking not liable for such losses. In practice, however, the banking as often adopted voluntary codes which specify that customers who sses are compensated – unless there are clear indications that they lluded in the fraud.

understand how the cost of fraud influences security decisions, it is nt to look at some of the available numbers. The United Kingdom ably the best data available. APACS, the UK payments associations, es numbers based on actual banking data, not estimates based on and extrapolation. As one would expect, direct losses from phishing the United Kingdom have risen, though with a recent fall: from 2 million in 2004 to GBP 33.5 million in 2006 to GBP 22.6 million (APACS, 2008). Over the past years, the number of phishing attacks eased significantly: from 2 369 attacks in 2006 Q1 to 10 235 in 2008 e broader fraud category of "card-not-present" fraud – which phone, Internet and mail order fraud – has risen from GBP 150.8 in 2004 to GBP 290.5 million in 2007.

to downplay the seriousness of these losses, but it is important to hat the damage of phishing attacks is still well below the numbers r fraud categories, such as stolen or lost cards (GBP 56.2 million in nd counterfeit card fraud (GBP 144.3 million in 2007). Furthermore, ese numbers are going up in absolute terms, so is the number of rs banking online, as well as the overall volume of online ions. APACS argues that the rise in card-not-present fraud should be against the increase in the use of online or telephone transactions. raud has risen by 122 % from 2001 to 2006, the use of online or e shopping itself has grown by 358 %. Unfortunately, the available

ounted for 40% of cases. PayPal recently reported their direct losses being 0.41% of overall transactions, but could not give information end of their losses (House of Lords 2007b, p. 196).

d implementation of security measures

le exact figures are hard to come by, the companies we interviewed their security investment levels are much higher than their direct sses, often by one or two orders of magnitude. The capacity to deal cidents is often already more expensive, let alone all of the ory measures and security defenses being put in place, such as the tion of two-factor or three-factor authentication.

reason for this level of investment is that direct losses are not seen sentative of the overall problem. It would be much more devastating, mple, if online fraud eroded customer trust or slowed down the f online financial services. Furthermore, there are reputation effects s that are targeted by attackers as well as for the industry as a whole. has robust estimates on either of these effects, which makes it for financial companies to calibrate their security investments.

general, the incentives are to keep fraud at acceptable levels and sate victims, rather than to eliminate it. The latter would be ically inefficient, not only in terms of direct cost but more ntly because pushing fraud back further might require the tion of security measures that make the use of online financial less attractive to customers. A reduction in the growth of the online ion volume is likely to imply higher costs for banks than the current caused by online fraud.

npanies, alone and through sector-wide collaboration, assess risks pare new security measures, which can be rolled out when they feel ent defenses are no longer adequate. Exactly when is hard to specify novations have been put in place rather quickly. Phishing attacks, mple, are increasingly dealt with by contracting out response efforts ity providers who scan for phishing spam and hunt down sites that e the official bank website, at which time they initiate notice and n procedures. Occasionally, this takes down legitimate web banking well, when the security department is not aware of a marketing e from another part of the organisation and thus has not whitelisted

ntal changes to their two-factor authentication systems, which are y easy for the attackers to defeat. More structural measures, such as ion authentication or three-factor identification, would require costly ations to the back-office systems, as well as requiring customers to w and more laborious security methods.

far, the response has been to make minor revisions to existing so as to disable the last successful attack tactic. These measures are companied by a number of other safeguards – such as temporarily down the processing of real-time transactions. The direct financial f each attack have been relatively low, which makes the possibility her successful attack less unpalatable. Ironically, one interviewee ed that the relatively modest losses per incident appear to be a te strategy of the attackers. These attacks are trying to stay under the the fraud detection systems – as well as making it less worthwhile enforcement officers to devote a large amount of resources to down the criminals.

ry of incentives for financial service providers

incentives of financial service providers are such that in many cases panies compensate customers for the damage they suffered from raud. They are willing to internalise these costs because the benefits veigh them. In that sense, they internalise the externalities of sub- security investments and behaviours of their customers, as well as ware vendors whose software is exploited to execute the attacks. wees told us that when designing the security of their services, they assume that the end user PC is compromised. Many financial service s claim they compensate all malware related losses. If that claim is , then the security level achieved by the whole value net may not be from the optimum. The financial institutions bear the externalities, are also in a position to manage the risk through their security s on online financial services.

ey considerations

lete information on customer trust

t, one could argue that there are still externalities in the sense that

ervices and, more to the point, from the increased adoption of these
In other words, this is a problem of incomplete information, rather
misaligned incentives.

lete compensation of fraud losses

econd consideration is that not all fraud-related costs to customers
mpensated. While the financial institutions compensate victims for
rect losses, this might not cover all the losses that result from the
n cases of identity theft, victims may not get all costs reimbursed and
y struggle for years with the consequences of having their personal
tion abused, such as blemished credit reports (TechWebNews,

y liability to merchants/customers

rd, in several countries the banking sector is re-considering the
liability regime, which might lead to "liability dumping". Financial
providers have already started to push more liability onto the
nts. It seems we might see a similar trend for customers. Late in
he Ombudsman for the German banking sector ruled against a
r who claimed to have been victimised by a Trojan, arguing that the
r provided no proof of a successful malware attack (A-i3 2006;
, 2006). The Ombudsman declared that the customer was not able to
evidence of a successful malware attack, even though the
r's machine was infected with malware. This appears to shift the
of proof onto the customer.

New Zealand, the banking association introduced a new code that has
t least part of the liability to customers. The new code allows the
o request access to the customers' computer to verify that the
g system, the anti-virus software and firewall were all up to date. If
ess is refused, or the computer is deemed inadequately protected, the
r's claim may be turned down. Shortly after it was adopted, the code
vere criticism. In response, several banks and other stakeholders
ed changes that offer more protection to consumers. Currently, the
seems to focused on the complicated question of determining just
rt of the responsibility lies with consumers (South, 2007).

development of what one could call 're-externalising' fraud losses

reason, a security official at a financial service provider called the to shift part of the liability to customers "a very dangerous path to

lising the cost of fraud

ically, the existing liability regime might actually be in the best of banks. By paying for, or internalising, the damages, whether l by law or voluntarily, banks have retained the freedom to balance l of security against other factors, most notably the cost of security s and the usability of online services. This has allowed them to ore cost-effective trade-offs than under a different liability regime. If ft more liability towards their customers, they then run the risk of more regulatory oversight for consumer protection.

interviewee told us that while the US banks fiercely opposed the ic Funds Transfer Act of 1978 since it placed all liability on them, ne many in the industry realised that the regime was actually ically more rational for them. He called it "a blessing in disguise". n (2007) found that during the period when the British banks l under a more lenient liability regime for ATM withdrawals than banks, they actually spent more on security, as they were doing 'due e,' rather than actual risk reduction.

ne financial service providers argue that the current practice of sating victims might provide a perverse incentive by rewarding rs for not securing their machine. Earlier experiences with ATM ggest the risk of such a perverse incentive is manageable (Anderson, should banks pass on the cost of fraud to customers and merchants – re potentially rising forms of damage that are currently not sated, such as the cost of recovering from identity theft – then this n the end lead to underinvestment, or even overinvestment, on the he banks, since they would be investing on the basis of due diligence han actual risk reduction (Anderson, 2007). In either case, the new es for financial service providers would shift the level, and type, of urity investments away from the societal optimum.

ndors

g software that includes malware. The software market is highly
tiated, although there are many linkages between segments, such as
g systems and application software. Nonetheless, each market
has somewhat different characteristics and hence creates different
es for software vendors to improve security prior and after release,
malware writers to exploit vulnerabilities.

ecent years, much has been written about the incentives for software
. The predominant view seems to be that software markets do not
ecurity. In the words of Anderson and Moore (2007, p. 7): "In many
, the attitude of 'ship it Tuesday and get it right by version 3' is
y rational behaviour."

t, some authors claim that security is a "market for lemons", as
ers cannot tell secure from less secure software. One interviewee
that he was in fact able to assess the security of the software his
ation bought, but that the different products were more or less the
terms of security. So there was no real 'secure' alternative.

ond, many segments of the software market tend to have dominant
cause of the combination of high fixed costs and low marginal costs,
network externalities and customer lock-in because of
rability and compatibility issues. "So winning market races is all
nt", Anderson and Moore conclude (2007, p. 7): "In such races,
tors must appeal to complementers, such as application developers,
m security gets in the way, and security tends to be a lemons market.
So platform vendors start off with too little security, and such as
ovide tends to be designed so that the compliance costs are dumped
nd users."

analysis provides a powerful explanation for how we got to the
state of affairs. Its implications are less clear for what happens after
e-to-market has been won by a software vendor. While any
sation is problematic, recent years have seen substantially increased
by many vendors to improve the security of their software. The
ment and deployment of vulnerability patches has improved.
y more important, the development of the software itself is
ngly focusing on security issues. Most of our interviewees agreed on
ey disagreed over the effectiveness of these efforts – some argued it
little too late, others thought the market was moving in the right

se of Microsoft

obvious reasons, one cannot avoid mentioning Microsoft in this The company's problems and efforts have been most visible. By e story is well known. Given the market dominance of its Windows g system, it has been a key target for malware writers. When the problems plaguing the platform mushroomed early this decade, tably in the form of global worm and virus outbreaks, Microsoft saw rced to change its approach. It all but halted development on its new g system and re-tasked many developers to work on much-needed improvements for its existing platform, Windows XP. These ments were released in 2004 as Windows XP Service Pack 2 (SP2). P2 contained many vulnerability patches, it also introduced changes ode base that set out to reduce the potential for vulnerabilities to be d. Furthermore, it turned on automatic updates and the Windows by default.

a variety of reasons, security among them, Microsoft then led the code base for what would become Windows Vista, the or to XP, at the cost of serious delays in the process. Vista's design ed better security principles, which inevitably led to numerous bility problems when hardware vendors and independent software had to adapt their drivers and programs to the new design. To a nt extent, the problems persisted even after the final release of Many would agree that these problems have slowed the adoption of s businesses and consumers wait for these problems to be resolved switching. All of this implies substantial opportunity costs for ft. There are no publicly available cost estimates, but it seems that the security-related costs of SP2 and Vista are anything but ven for a company of this size.

rosoft is not alone in this trend reversal, though it might be the most e example. In contrast, there are vendors who operate in markets that manded security from the start, such as the defense industry. These have developed along a different path compared to those in the nsumer market. As a result, their business models make it easier for o economically justify security investments in the software ment process. Just to be clear, the increased efforts in software do not mean the problem of malware is getting smaller, or even that uency with which vulnerabilities diminish is discovered. There is a

withstanding the different business models of software vendors, a
of incentives explain why this trend reversal took place. They point
omplex interplay between incentives and disincentives for security.
dings do not conflict with the incentives mentioned in the literature,
they confirm and complement them by focusing attention on the
es for established software vendors, *i.e.* after the "race-to-market"
n won

ves for software vendors

f vulnerability patching

eloping patches for discovered vulnerabilities is costly, even if the
f is not hard to write. As one senior software security professional
d: "It's like the Mastercard commercial – two line code change, 20
, finding every other related vulnerability of that type on every
product version and all related modules, fixing it, testing it, 3
Giving the customers a patch they can use that does not break
g, priceless."

ough it is daunting to calculate reliable and comprehensive
, the anecdotal evidence we were given suggests that an ongoing
of patch development, testing and release for a complex piece of
– like an operating system or an enterprise database system, which
of tens of millions lines of code – is easily measured in millions of

n more important, some interviewees argued, are the opportunity
tasking good software developers with vulnerability patching. One
wee said: "If you reallocate the developer time for patches to other
might not be enough to build a completely new product, but you
uild some complex functionality you could charge for. I could build
ng I could charge money for... if I did not have these defects to
te."

hing also imposes costs on the customer who applies the patch. This
lude the cost of testing the patch before deploying it within the
ation, the actual deployment for all the relevant systems, as well as
s of remediation when the patch turns out to "break something" –

there are indirect effects that do affect the vendor. First, patching he maintenance costs of the software, which can be considered o raising its price and thus lowering demand – although this effect is ntly mitigated in the case of lock-in effects or lack of alternatives. nterprises assess the so-called "total cost of ownership" of software, an just the price of the licence. It is not uncommon for maintenance be much higher than the price of the licence itself. Second, if is too costly for customers, they may not keep their machines ly patched. The resulting security problems may tarnish the on of the software itself – we return to brand damage and reputation hortly.

for enterprises vs. home users

esponse to these effects, many software vendors have set out to he costs of patching for their customers. For enterprises, patching is nt issue than for home users. The former need to have more control e deployment of patches as patches potentially disrupt critical . In some cases, they might opt to not apply certain patches. "While be wonderful if everyone stayed fully updated all of the time," said rviewee, "many enterprises choose to do extensive testing first, to avoid blackout periods, and take into account many other ations specific to their business before an update can be deployed. ses that regularly deploy updates will be less vulnerable to malicious so with all of that in mind, each business must make the risk trade- is appropriate for them."

vendors we spoke to described efforts to better support their customers in this regard. Microsoft, for example, introduced s Server Update Services (WSUS), which allows IT administrators ol the deployment of patches across the computers in their network nore, vendors try to improve the information they provide with so that businesses can make an informed risk assessment regarding and how to deploy a patch.

eral interviewees also indicated that enterprise customers asked for patches, which are tested and released together on a regular e (e.g. weekly, monthly or quarterly), rather than single-issue fixes released as soon as they are ready. "We do not do single fix patches,

home users, reducing the costs of patching has mainly consisted of
ing easier, more user-friendly mechanisms to deliver and install
Microsoft developed "Automatic Updates" and turned it on by
in XP SP2. The vendor reported that over 350 million Windows
s worldwide receive the monthly "Malicious Software Removal
rough Automatic Updates or Windows Updates (Microsoft, 2007).
nvironment of open source software, Firefox – an Internet browser
second-largest market share, after Microsoft's Internet Explorer –
bled automatic updates by default since version 1.5. Rather than
g patches, the developers of Firefox release the patches as soon as
ready. The default setting of the browser is to download and install
the earliest opportunity. The developers recently reported that under
v model, 90 % of Firefox users installed a recent security patch
nx days (Snyder, 2007).

ing always required?

costs of patching could also work as a disincentive for those
vendors seeking to avoid these costs. As a result, vulnerabilities
un-patched for too long, assuming they get patched at all, or the
of the patches might be too low. The urgency of this issue increases
kers, as has been reported, are moving way from exploiting the
g system and toward third-party applications and hardware drivers
2006).

wever, not providing vulnerability patches does not seem to be a
strategy for an established vendor whose product is actively being
by malware writers. On the other hand, even substantial efforts in
evelopment can leave a software product vulnerable – *e.g.* because
are more complicated to develop and test for products that are
ntegrated into a larger software package. An analysis of the known
bilities for Internet Explorer found that for a total 284 days in 2006,
as exploitable code available for known, un-patched critical flaws in
Explorer 6 and earlier versions (Krebs, 2007).

vendor's market position requires it to perform costly patch
ment, then these costs might provide incentive for more investment
ity early during the development process. This would be done in the
reducing the number of vulnerabilities after release – or perhaps

g vs. secure software development

le vulnerability patching is generally seen as desirable, although not yone (Rescorla, 2004), many have argued that it does not really solve erlying problem. Finding and patching vulnerabilities might not e software product itself more secure. Some research suggests that y products, the discovery rate of bugs is more or less constant over n other words, finding and fixing a vulnerability does not reduce the of an attacker finding a new vulnerability to exploit (Rescorla, urthermore, patch development consumes resources that could have ed to make software more secure before it is released.

is a valid criticism. However, several interviewees made the case tly patching procedures still provide an incentive for more up-front ents in secure software development. One argued that the more l incentive for secure software development is the fact that back-end costs are much higher than the costs of preventing the vulnerability development. Another interviewee told us: "The argument to make ng better code is cost avoidance, even if you charge for support (and The way you get a good margin on it is if you can charge for ance but you do not have to constantly produce patches because e expensive, that cuts into your margin."

did not come across economic analyses that directly compare the secure development with those of patching. It is unclear whether even have this kind of data available. One interviewee told us: "I add up what we've spent on the front-end. Most of secure ment is good development, not some special security add-on."

eems clear, however, that the costs of secure software development tantial. It requires more resources and can affect time-to-market of a oduct – a critical factor in many software markets, though here too ct may be tempered by customer lock-in. Furthermore, secure ment often involves costly assurance processes. One interviewee d the so-called "Common Criteria" evaluations for major releases of oducts. These evaluations are made by external consultants and were d to cost between USD 500 000-1 million each – not including the nsuming involvement of internal staff.

n in the absence of hard numbers, the interviewees were adamant re are significant cost savings to be made by investing in secure

ns in opportunity costs that potentially are even higher In the words interviewee "I worry about the opportunity cost of taking good ers and putting them on tasks for security patches for avoidable, ble defects That's why we put a lot of work up-front to avoid that e training, we have automated tools – anything you can do earlier in e is goodness It's never been hard to justify those costs"

brand damage and reputation effects

additional explanation for the increased security efforts of software are the reputation effects that they suffer for poor security – or or good security The strength of these effects are notoriously to estimate Some have suggested that they provide a fairly weak e (Schneier, 2007) Whether that is true or not, it does seem to play a e major security-related changes within Microsoft were driven by or worm and virus outbreaks in 2002 and 2003 The key difference those security incidents and ones that preceded them was scale and lting damage Neither affected Microsoft directly The reputation f those incidents seems to be the most plausible explanation for the in the company's course

mentioned earlier, Microsoft has invested in mechanisms to make it or its customers to patch their machines, even though they do not e customer's patching costs directly Furthermore, so far Microsoft wed pirated versions of Windows to download security patches This to value the reputation of the platform more than denying services to tomers Keeping their customers patched as much as possible helps e the scale of security problems that the platform is associated with

incentive of reputation effects might be stronger in open source nities, where reputation is a very valuable resource (*e g* Watson, t might help to understand why early in the development of what become the Firefox browser – shortly after the code of Netscape nicator had been open-sourced in 1998 – the developers made a of security-conscious choices The security performance of the played a key role in the positive evaluations of software reviewers

re vendor trade-offs and disincentives

ing functionality

rt of the reason for the mess is that people want fancy gadgets and do
as much about security, and that's exactly what they got," one
security professional told us. The 'gadgets' referred to in this
nt are the functionalities provided by software products. Even
with an established market position will at some point want
rs to buy a newer version of their product or a complementary
Another interviewee said: "No-one buys your product only because
ure, they buy it because it allows them to do new things." The drive
market to produce ever more powerful software has generated
is innovations. At the same time, it has made it much harder to build
oftware.

ctionality versus security is not necessarily a zero-sum trade-off.
nctionality can be security related, for example, or it might be
ented securely. In practice, however, they can be difficult to
e. The history of software development is rife with examples where
fs in the design of software have favoured functionality over
Many of the much-maligned features of Microsoft's Internet
r, such as its deep integration into the Windows platform, started out
ionality – *e.g.* the ability of a website to silently install code on a
ystem, which would increase the functionality of the system without
g the user to understand and manage the process of installing
There have been many beneficial uses of this functionality, but it
turned out to be a huge security risk. In response, IE7, the latest
of Internet Explorer, has reversed many of these design decisions.

re is an intrinsic tension between adding functionality and making
more secure. Security benefits from simplicity and a limited
of code (*e.g.* Barnum and Gegick, 2005; Bernstein, 2007). Many of
major software products are neither. The need to expand
ality with each release only exacerbates the situation. Of course,
oftware development practices set out to mitigate this problem, by
g the "attack surface" of a certain functionality and manage the
ng risks or, if the functionality is inherently insecure, to exclude it
product.

Box 5.1 Microsoft's Vista: An attempt to balance compatibility and security

g the development of Vista, Microsoft decided to change the default way ounts were set up. This required Microsoft developers to create a viable user mode with restricted privileges. They introduced User Account UAC) for this purpose. Their enterprise customers, many of whom wanted eir desktops under standard user accounts, applauded this development, as it l to reduce their total cost of ownership. The problem was that it created ompatibility issues with the existing third-party software, much of which umed administrator privileges. While vendors were informed about the g changes, many did not actually adapt their code to work with these One interviewee explained that it was not attractive for vendors to comply new restrictions, because they had to invest in changing their code just to me functionality that they already had before Vista.

Vista was released, a substantial number of these compatibility issues were ed, even though Microsoft itself developed auto-mitigation measures to deal ny application compatibility problems that the vendors did not resolve es. Users experienced poor or missing device drivers and incompatible programs. Many complained about the constant security prompts and that UAC confronted them with. Because many programs did not run in standard user mode, they constantly had to ask for elevated privileges, ggered the UAC prompts. This was exacerbated by the fact that UAC was emented very elegantly and thus generated more prompts than needed. As rviewee explained, the move to UAC "is considered a paradigm shift that late into worse user experience if the user is running software that has to very day."

soft anticipated these problems to a certain extent. They felt that the bility problems of end users were worth the price of moving the software toward building products that could operate under a standard user model out a way to force the third-party vendors to adapt their software, this would ngerous game to play," said one interviewee, as Microsoft itself will receive e blame for these problems. UAC is one example.

security improvements in Vista suffer from the same incentive problem y work if the independent software vendors adapt their code. If using the feature is not turned on by default, the vendors might simply ignore it, eans that the feature does not actually improve security for end users. If the turned on by default or if it cannot be turned off, then users will experience compatibility issues. These compatibility issues likely translate into a d adoption of Vista, especially by enterprise customers, as they wait for oblems to be sorted out before they move to the new platform. For

could argue that as the security-related costs of users go up, the
will reward security-related functionality that can reduce those costs
re several well-known counter-arguments to this – including lock-in
lack of alternatives, weak market signals for security and the
tion asymmetry between vendor and customer That said, there
to be a market demand for certain security improvements, most
those that reduce the total cost of ownership Some software
, both proprietary and open source, are actively marketed as being
ecure and less costly to maintain than their alternatives or
ssors Whether the market over time can distinguish between empty
nd security improvements that actually achieve cost-savings is not

g compatibility

discussed above, software products benefit from positive network
ities The value of a software platform – such as an operating system
ses non-linearly with the number of users There are two sides to
e more users there are, the more vendors will want to develop
e for that platform, and the more software there is for the platform,
e users will want to adopt it Anderson and Moore (2007, p. 5)
ed that all of this implies that platform vendors will impose few
restrictions so as to appeal to third party software vendors – *i e* to
n compatibility and inter-operability of software How these
es play out of for a specific vendor depends on the type of product
vide and the position they have in the market

a dominant platform, maintaining compatibility is key when moving
e version to the next As one industry insider told us: "The only
Microsoft] cared about in the transition from Windows 95 or
s 98 to Windows XP was application compatibility, otherwise
would never move to XP." This had all kinds of effects on security
problem of malware

achieve maximum compatibility, the default installation of XP set
ser up with administrator privileges, which means that people
y operated their machine under a user account that allowed
cted control over the machine From a security standpoint, this is
able, because it means that once a machine is successfully attacked
use, malware has full access to the machine and can, for example,

the "attack surface" – *i.e.*, the amount of code, interfaces, services, ocols available to an attacker.

esponse to the default user setup of XP, third-party vendors assumed isers would run with administrator privileges and they designed their is accordingly. In turn, because so much software assumed the user administrator privileges, running the system as a regular user with privileges was not really viable. "The end user was pretty much o run as administrator", said one interviewee. While they might not uch of a choice, end users were accustomed to having full control ir machine, unbothered by security restrictions.

ge organisations did sometimes set up the desktops of their es with restricted regular user accounts. This is a costly set up, r, because it requires a lot of support staff to manage these ions. Even minor changes needed administrator privileges and thus a staff action. Of course, if you set up your users as administrators, the costs are also high, because of the increased security risks. The only break out of this self-reinforcing costly path is for everyone to adapt haviour.

g for user discretion

issue that runs throughout the challenge of software security is user on – that is, key decisions about how to configure and operate the product are left to the user. The user – or in enterprise contexts, the nistrator – decides whether or not to install vulnerability patches, the ides whether to operate within User Account Control or to turn it user decides how to configure a firewall, and so on.

r discretion allows software products to be adapted to a wide variety xts and user preferences. That means the product can reach a wider and can create more benefits for its users, making it more valuable. more importantly, user discretion touches on property rights. e runs on machines that are not owned by the vendor. In principle, owners who should be able to decide how to balance trade-offs functionality, performance, availability and, yes, security – as well ther value relevant to them. After all, the owners are the first to bear for what their system does – whether this affects themselves when eployment breaks critical business applications, for example, or

h user discretion comes user responsibility. This is a blessing and a
r software vendors. The blessing is obvious: many of the current
problems fall within the realm of user behaviour rather than within
m of software production. This shields vendors from part of the
bility to resolve these problems. Of course, it is also a curse. The
s that users make affect the security performance of a product,
n turn affect the reputation of the product and its vendor. There is
of evidence demonstrating that in many cases, users lack the
tion or expertise needed to make rational security trade-offs or that
cisions do not account for the costs they impose on others –
g, but not limited to, reputation damage to the software vendor.

re are limits to user discretion. There are hard limits, where software
does not enable or allow you to take certain actions, and softer limits,
he default configuration of a product tries to guide behaviour in a
direction. For example, when Microsoft introduced UAC, it turned
ure on by default, but it did include the possibility to turn it off by
g the system settings. Preliminary feedback indicates that, so far,
ee quarters of users keep UAC turned on.

ere and how to set such limits is a difficult balancing act for vendors.
es many trade-offs between user discretion and protecting the
and reputation of the product. As one interviewee explained:

at debate raged on for four years straight, from the team level to the
VP level and we rehashed that debate fifty times in those four years.
ow – what should the defaults be and how much pain can we put the
to get through to the independent software vendors? Are we being
essive with this plan or are we not aggressive enough? It was a huge
ring decision that really took a lot of guts at the VP level to support
we knew we were going to generate some customer dissatisfaction.
alternative is to say, I hope anti-malware engines can keep up with
."

ry of incentives for software vendors

ware vendors work under a mixed set of incentives, which may vary
erent market segments. They do experience increasing costs as a
f growing security problems, most notably the direct and indirect
patch development and reputation effects. That explains why many

net effect of the mixed set of incentives is dependent on the product market segment in which the vendor operates. Assuming all other re equal, the increased efforts mitigate software-related security s. However, at the same time as security efforts are being increased, is becoming more sophisticated, adapting to the new defenses standing the efforts of software vendors, many of our interviewees d that the situation would get worse still, before it would get better.

dors do not bear the full costs of software insecurity – *i.e.* there are ities. Schneier (2007) has repeatedly argued that all the money that ers of software products are spending on additional security products vices should be counted as externalities generated by those software . That might not be fully correct and it may overestimate the size of lem.

a certain extent, security problems are connected to users' decisions haviours – as is inevitable, given user discretion over the ation and use of software, as well as social engineering attacks do not need software vulnerabilities to compromise a system. If dy decides to buy a cheap or highly functional software product with security problems plus separate security software, it is that er's choice and this should not be treated as an externality. In theory, unctioning market would offer software with different degrees of on and let consumers choose. However, that assumes that everybody information and that there are no externalities on the consumer side know, in many software markets consumers experience lock-in or a lack of alternatives. So there are externalities generated by the ' decisions, but they are probably lower than the total cost of measures.

ustrars

Domain Names System (DNS) is part of the Internet infrastructure, uch it is affected by malware in a variety of ways. There have been ublicised botnet-assisted denial of service (DDoS) attacks on root and TLD name server operators, aided by sophisticated tactics that the existing DNS infrastructure to amplify the attacks.

ddition to the threats to the DNS infrastructure posed by malware,

by security service providers working on their behalf, often assisted
rt volunteers working at ISPs, CSIRTs and other organisations.

procedures to take down phishing sites are changing constantly, as
s adapt their strategy in response. Typically, ISPs and registrars are
d in taking down a phishing site. The first takes down the hosting
while the latter removes, suspends or redirects the domain names
the attackers. Redirecting a domain name means sending the traffic
her location, typically to allow law enforcement or security
sts to examine it more closely.

pension is sometimes preferred over removal, as the latter would
ne attacker to register the name again elsewhere. The response of
d registrars to the notification of phishing sites varies. Some act
others do not. At the latter extreme, we find bullet-proof hosting,
usiness model is based on non-response and keeping malicious sites
as long as possible. Research suggests that legitimate ISPs and
s, once they are under pressure to act, go through a learning process
elop procedures to deal more swiftly with abuse (Clayton, 2007). At
nt, the criminal activity starts to migrate to other, easier targets.

transaction costs of domain name registration itself are very low –
nced by the practice of "domain tasting", where millions of domain
re registered, the overwhelming majority of which are cancelled
he so-called "grace period" expires. For the registrar, this process is
le because it enables a business model to find profitable domain
hrough trial and error, which drives up the number of registrations
make it past the grace period and thus generate revenue. Some
wees suggested that there is a relation between domain tasting and
, but within the context of this study we have been unable to find
to clarify and corroborate that relation.

ves of domain registrars

incentives of ISPs were discussed earlier. What about the registrars?
gnificant extent, ISPs and registrars are overlapping categories.
name registration is an extremely low margin business, which is
any registrars tie them to complementary conventional ISP-type
, such as web hosting and hosted e-mail services. Some registrars
er domain names at a slight loss, in order to entice people to register

overlap between registrars and ISPs means they share similar es. It also means that the size of their operations is such that staffing e desk and other security-related positions is seen as a normal cost of usiness. The different parts of the business often share a centralised esk. Furthermore, they need such capabilities for other reasons than urity, most notably to deal with complaints regarding copyright ment – our interviewees reported that the latter made up a large of the incoming complaints.

course, there are also smaller registrars, with or without nentary services, who lack staff to deal with abuse – again, similar to ation with ISPs. Some of these smaller registrars leave it to the provider to deal with all content-related complaints. Because of the between registrars and ISPs, we refer back to the section on ISPs to nse of the incentives that both have in common. We only briefly ise them here, complementing them with more specific findings for s.

f customer support and abuse management

with any business in a competitive market, registrars have an e to reduce operating costs. This includes customer support and anagement. The number of complaints was reported to have risen ually in recent years, though part of this growth coincided with of the customer base. At the same time, the response process has partially automated and thereby more efficient. To illustrate, one wee reported getting 1 200-1 500 incoming complaints per day for a r base of several million. Only a minor part of the overall incoming ions relate to malware. The bulk consisted of complaints about copyright violations.

le the company in question offered complimentary services, most of oming complaints were about domain names that were registered them, but hosted elsewhere. They were contacted because their service did not allow the domain to be used for any kind of abuse – y have a reputation for enforcing these terms. On the whole, the wee estimated that they suspend around 20 domain names per day se-related reasons. Only a few per week were specifically for . One explanation offered for this relatively modest number was end users who were infected by malware, it is often difficult to tie

ation therefore provides an incentive that, all things being equal, gainst security This is reinforced by the need to investigate the ion, to understand whether the domain name is indeed associated dicious activity Given the dynamic and increasingly sophisticated s of phishing gangs, this can be more difficult than it may seem at nce Even for the experienced staff at larger registrars, investigating cation and request to suspend a domain name for malware-related an take several hours Phishing sites are less difficult to investigate typically be dealt with within an hour

incentives for criminals are to register with registrars who are slow nd to abuse The longer the domain name stays active, the more ul their attack can be This means that not all registrars are equally Those that are swift to suspend, remove or redirect a domain name y incentivise criminals to look for easier targets Given the enormous of registrars, both for generic and country-code top-level domains, r target is usually not hard to find These registrars do experience ences for their lack of responsiveness, similarly to the consequences 's suffer In that sense, the costs of customer support and abuse ment work as an incentive to improve security

interviewees explained that it was their experience that if they dealt ely with abuse, then criminals would avoid them or move elsewhere, educed the amount of complaints coming in, as well as associated ch as blacklisting The amount of abuse had gone down relative to vth in their customer base

f blacklisting

registrars offering hosting and e-mail services are subject to the blacklisting along the same lines as the ISPs Blacklist operators tch registrars and their responsiveness to abuse complaints In cases, blacklists may be directed at the registrar itself A case in the recent row between the blacklist operator Spamhaus and the registry/registrar Nic at Spamhaus had requested Nic at to remove domain names it said were associated with phishing by the "rock gang Nic at did not comply with these requests, citing legal nts They argued that they could not legally remove the sites, unless us provided them with clear proof that the domain names had been d using false information (Sokolov, 2007)

o a symbolic listing – no longer actually blocking the IP addresses, ing them listed as "spam support." Several of the offending domains en removed, but Nic.at denies that they complied with the request imes that the hosting providers took action (ORF, 2007, Spamhaus,

f brand damage and reputation effects

re also appear to be reputation effects, which provide security- ng incentives. As mentioned earlier, there are several cases of s who were popular among phishers and who at first did not respond ests to suspend domains. Then they apparently went through a process and started to remove domain names quickly in response to (Clayton, 2007). It is unclear what precisely prompted this learning but their behaviour suggests that the registrar does not want to be ed with the malicious activity.

other case is the ccTLD of Tokelau, an island with 1 300 inhabitants rritory of New Zealand. The registrar for the .tk domain is a Dutch- n company, which hands out most domain names for free, making from showing advertisements on the registered domains. After announced that over 10% of the .tk domains were suspected of s activity, the registrar introduced new measures, which included scanning of the domains for malware (Dot-TK, 2007).

s of maintaining reciprocity

registrars, maintaining reciprocity is as important as it is for ISPs. rd numerous examples of registrars with hosting and e-mail services ng instances of blacklisting through informal contacts with blacklist s as Spamhaus as well as major e-mail and network providers. One wee mentioned that one direct benefit of being responsive to abuse nts is that it typically keeps sites with security problems off ts – or at least ensures a proportionate response from blacklists, such g the specific machine associated with the abuse, rather than listing a nge or subnet in which the offending machine resides. A security t an ISP claimed that his organisation sponsored Spamhaus, which ely gave them a free pass in terms of being blacklisted.

interesting new example of reciprocity stems from the size of the

n registrar disincentives

tsks and constraints

with the ISPs, a number of legal ambiguities surfaced which in some anslated into disincentives for security. Some interviewees argued l to be careful with monitoring the hosted sites on their network. One wee said:

e legal liabilities kick in as soon as you have knowledge or should nowledge that something took place on your network. If you are ely monitoring all the content of your hosting customers but for r reason something is missed, while there is an expectation that you have caught it, then you could potentially be held liable for that. So the monitoring that we do is somewhat limited in scope and only to areas where there is some sort of a safe harbor legal provision."

n there are potential liabilities around suspending or removing names, as it involves a contractual relation between registrar and it. Even if the terms of service of the registrar preclude the domain eing used in relation to spam or other forms of abuse, that still the registrar to investigate and build a case showing that those terms en breached. That can be costly.

eral interviewees in the security community pointed out that security onals often use a short cut rather than asking the registrar to ely investigate and decide on an abuse complaint, they point out that strants WHOIS information is false. As one interviewee explained: ose registrars that are not willing to assume the risk of the liabilities, OIS accuracy policy is a comfortable refuge." Referring back to the Spamhaus vs. Nic at, the request of Spamhaus was indeed to suspend hing domains on the grounds that their WHOIS information was he response of Nic at was that they were contractually bound and o remove the domain names unless Spamhaus could provide legally gful evidence that the WHOIS information was indeed false.

re is also the risk of collateral damage from removing domain. It could be that the domain name is indeed used for phishing, but that activity associated with it is criminal or that the actual owner is of what is going on. The fact that the registrar acted in good faith e request of others would in all likelihood not shield it from liability.

ecord for the security website SecLists.org at the request of
e.com, after the security site published a list of 56 000 MySpace
es and passwords that had been circulating on the Internet (Utter,

n if the domain is actually owned by criminals, that does not mean
strar is shielded from repercussions. In the past, there have been
spammers successfully suing their ISPs for shutting them down, just
have sued blacklist operators such as Spamhaus – a case which was
won by the spammer, although that did not affect Spamhaus directly
it is located outside the courts' jurisdiction. In short, the risk of
drives up the costs of compliance with abuse notifications,
ly in combination with more complicated and difficult to diagnose
rategies, which work against security.

everyone agreed that these liabilities form a significant risk. "In a
ases the risk of incurring liability vis-à-vis a spammer or malware
s very minimal," said one interviewee. "I believe most registrars
on that premise. Certainly, I have heard the excuse of liability used
registrars and I feel that it should not be used to absolve yourself
ur responsibility to your customers and your community. The real
he cost of defending yourself against court cases. Even in the most
is cases there is some exposure and you need to take those exposures
ount into your business model."

y and customer acquisition

rviewees expressed mixed views about the relationship between
costs and acquiring and retaining customers. The dominant view
d to be that proactively fighting abuse actually helped to acquire and
ustomers, as it helps build their brand as trustworthy and secure. In
, active abuse management helped the registrars to mitigate risks of
ting, also for customers that were not directly involved in the abuse
Non-responsive registrars and hosting providers might experience
vere forms of blacklisting which are correlated with substantial
l damage within their customer base.

other side of that story is that proactive abuse management often
swift action, which might be perceived as hasty or unjustified by the
rs involved in the abuse issue. The latter might see themselves as

ary of incentives for domain registrars

istrars face a mixed incentive structure for security that varies across rent business models To the degree that registrars operate as ISPs – ny do, as they tie in registration services with hosting e-mail and omplementary services – they face a similar incentive structure some evidence that suggests that registrars are indeed responsive to pressure and that improved security provides benefits (*e g* Clayton,

ecurity officer at an international bank told us he was not worried he fast-flux networks for phishing, because in his experience s were quite responsive in addressing the attacks at the level of the name That still implies, however, that in the absence of outside , the incentives for security are not strong In light of the large of registrars currently in operation, this suggests a long learning even if we assume that registrars that have improved security will back into complacency

was discussed earlier, the abuse complaints that ISPs receive cover fraction of the actual amount of abuse on their network. The wees confirmed that this is similar for the domain names or hosting that fall under their purview "For every abuse situation we are about, there are probably several more going on that we do not get about," said one interviewee In practice, this means that while gistrars may have incentives to improve security, their efforts do not he full extent of the security problems associated with their services r customers In other words, there are externalities arising from these for other market players in the value net

users are arguably the most heterogeneous set of market actors, from average home users to SMEs to public institutions to global ions Rather than trying to differentiate all of these actors, we iscuss two extreme categories – home users and large organisations, nd private – and discuss in general terms the incentive structures hich they operate

s themselves. That incentive structure has changed dramatically. By its presence to the end user, malware can turn end user machines ack platforms to be used against many other players in the tion network.

lack of home-user action against the infection of their machines is a ation of:

ncomplete information – not knowing that they are infected or nable to evaluate the relevant security risks and defense strategies, and

Shortage of incentives: home-users do not have to bear the costs of heir decisions on other market participants.

mplete information is important, because it further weakens the misaligned incentive structure. While it is true an infected machine mobilised for use against other actors than the machine's owner, it is y also true that a significant portion of malware poses a direct threat wner – for example, keyloggers that capture access codes to financial s, 'ransomware' that renders user files inaccessible until a ransom is he criminal, or Trojans that enable man-in-the-middle attacks during online banking sessions.

rinciple, these risks could provide a strong incentive for home users e their machines. But their lack of understanding of such risks or defend against them renders the incentive to act on them rather weak, nexistent. The interviewees at ISPs told us that when they contact hose machines have been compromised, the response is generally sitive. Their customers had no idea what was going on. Once it is d, they are often co-operative.

he abstract, however, the information about risks is not getting . A security officer at a smaller ISP explained it this way: "At any oint in time, we have 600-800 customers who have a malware, abuse ity problem with their machine. You do not see those numbers in the ecause a journalist does not think this is a problem, 600 out of 400 tomers. This is also why end users do not think it is a problem, the chances of being hit seem so low."

cost of increasing security provides a further disincentive. The ess to pay for security services seems low. As quoted earlier, one

ere was still a large group of people not installing the software

milar phenomenon was related to us by the head of Internet security
e ISP: they too offered an AV solution as part of the subscription.
e people who did install it often did not keep it up to date. He
it on poorly designed software. That sentiment was shared by a
tative of a consumer organisation. "We see that the products
ers get for establishing some degree of security for their PC do not
operly, and they are too complicated to manage. Consumers cannot
their own security given the tools they are provided with." When
hether in their view consumers would be willing to pay for better
, the interviewee responded

general terms, they do and they do not. They just expect it to be the
setting. Most products are secure. When you buy a car, it's got seat
r bags, brakes. Those things are included in the product. Consumers
charging extra for that is a bit ridiculous."

ne with these views, a survey by a consumer organisation found that
ority of their members felt that Internet security was a shared
bility – the consumers themselves are responsible for their online
ur, but the technical aspects of security are the responsibility of
most notably their PC retailers, ISPs, software vendors and the
ment (Consumentenbond, 2006)

difficult to disentangle incentives from incomplete information, but
mbined effect is to undermine the willingness, as well as the ability
Often this situation is described with a sense of inevitability, as if the
ser is a static entity with no learning curve. Surveys suggest that
incorrect.

ne users are adapting their behaviour, but it is unclear how these
add up, how to connect the disparate, if not contradictory, pieces of
tion from the plethora of surveys out there. Even if we ignore the
ancies between the numbers, it is hard to characterise the current
. Surveys tell us a large number of people are worried about identity
ivacy, security, online predators, fraud and other problems. In fact, a
nt portion of people are turning away from the Internet altogether
eOnline, 2006). At the same time, adoption of security measures
firewalls and AV software is increasing, slowly but surely (Fox,

ve structure for home users

key question regarding the incentive structure is: how, if at all, are sers confronted with the costs generated by their security trade-offs? se, technically, they are confronted with them all the time. The bulk spam messages that everyone receives is sent through botnets, to it one consequence. But the causality between individual behaviour h aggregate effects is too abstract and complicated to have a k effect.

dback typically stems from actual security problems that people nce – the victims of fraud, identity theft or, less dramatic, degraded ality of their machines. According to a 2007 survey by *Consumer*, 1 in 5 people experience a major virus problem, 1 in 11 experience spyware problem and 1 in 81 actually lost money from an account ners Union, 2007). Assuming these numbers are correct, that would omewhere between 20-30% of all home users have directly nced the consequences of their security decisions. Potentially, this a powerful feedback loop, but the unanswered questions are:

v do people understand these incidents? Do they relate them back to vn decisions? Do they have adequate tools and capabilities to act on derstanding, assuming such tools exist for end users? (The existing software suites are increasingly ineffective in detecting malware.)

most direct mechanism (which is currently internalising some of the ities generated by end users) is the ISP practice of isolating infected ntil they resolve the security problem. It would appear that this works for relatively modest numbers of infected machines, but, as r experts say, it does not scale to the actual number of infections.

not just ISPs that bear the externalities generated by home users. nline businesses are confronted with botnets and related security and they have to provision their services accordingly – whether they commerce company buying DDoS mitigations services from its ISP, nline bank that has to design its services under the – all too valid – ion that the customer's machine is compromised. Few of these parties are in a position to mitigate these risks by influencing the trade-offs of home users. Thus, defending against these security s perceived as the cost of doing business.

to understand the security risks they face, take precautionary
s, as well as build incident response capabilities. Notwithstanding
dvantages, research often reports that both public and private
ations underestimate the risks they face or under-invest with regard
rity. Some of our interviewees reported compromised machines in
tworks, which they perceived as more or less inevitable. They
d that their networks were by necessity rather open to accommodate
ors, or the flexible use of services throughout the organisation. One
wee said his network was like a fortress that kept intruders out, but
meone had gained a foothold inside, there were many opportunities
cious activity.

le interviewees reported instances of malware on their network, they
this malware to be generic and not targeting their organisation
ally. It is unclear how valid this claim is. The way they found out
ese compromised machines – *e.g.* through notification by security
providers which were not under contract with them, or during the
s of support desk staff repairing malfunctioning machines – suggests
r risk perception of malware is not based on any formal type of
of their own services and networks.

re are many known cases of companies who have suffered
ssing security breaches – and there are undoubtedly many more
n ones. That being said, it is rather difficult to determine the
ate level of investment in light of these threats. While more formal
instruments have been developed in recent years to support these
s, their application requires the input of values and probabilities that
hard to estimate with any degree of reliability. According to the
SI Computer Crime and Security Survey, less than half of all
tions use instruments such as ROSI, IRR and NPV (CSI, 2007).
e providers have very little actuarial data to base policies on.

le the security practices of large end users undoubtedly leave much
r improvement, it is also important to realise this: many of the
hat businesses underestimate risks and under-invest in security stem
search sponsored or carried out by security providers, whose
e is to overestimate the problem.

trast these claims with the findings from the CSI Survey, which
d decreasing loss estimates from respondents for five years in a row

versed as damages per reporting organisation doubled to USD 345
s difficult to assess whether this represents a one-time deviation or a
d reversal of the downward trend. Most likely, it reflects the
ogy race between the provision of cybersecurity and ever-more
cated and virulent criminal attack techniques. It is also important to
t direct losses are no measure of the complete financial impact felt
ty.

f the trade-offs

anisations face all kinds of trade-offs regarding their information
decisions, including malware. Take the issue of patching. We heard
s that patching mission-critical software systems can cost millions
reason, some companies did not patch immediately after release of a
bility patch, but waited for months and then applied several patches
neously.

re were even examples of organisations that consciously never
, estimating the risk of disruption to be higher than that of security
s. In the financial sector, security measures often face a trade-off
availability of the systems and their performance. In a world where
ity to process information in milliseconds affects the bottom line,
s that improve security but slow down transactions are not an
choice. A similar trade-off exists between security and availability –
he uninterrupted uptime of systems. All of these trade-offs involve
assessments of costs and benefits, often in the face of uncertainty
ing information.

re the externalities?

n if it is true that large organisations might not fully understand the
d benefits of information security, the more relevant issue is whether
ation causes market externalities. In the absence of externalities, it is
their purview to pursue whatever security strategy they deem
iate and bear the consequences of those decisions. In most generic
he answer is Yes, there are serious externalities.

mples of externalities are hospital records that are compromised,
l records of millions of citizens that are "lost," and a job website that
n compromised, allowing the personal information of over a million

will be implicated in a wider variety of security breaches than those already observed.

damage and other incentives

at are the incentives for these organisations to prevent these ities? There is brand damage. Organisations that have been breached trong incentive not to disclose this information. However, many US have adopted legislation that requires organisations to publicly security breaches. The legislation includes no penalties, but still strong incentives because of the prospects of public assment and loss of share value.

upbell *et al* (2003) reported that, on average, breaches of utiality had a significant negative impact, causing an average decline et value of about 5 %. A study by Cavusoglu *et al* (2004) also that announcing an Internet security breach is negatively associated market value of the announcing firm. The breached firms in the lost an average of 2.1 % of their stock market value within 2 days of ouncement — an average loss in market capitalisation of USD 1.65 per breach. While these effects are significant, some experts argue se are temporary and that, over time, the notifications will have less impact, as the number of notifications increases and they lose their lue.

a breach notification legislation enables other parties to hold the ble organisation liable for any damages they have suffered. This done by individuals affected, but perhaps more realistically by other ies that have more resources to pursue such a course of action. In the the security breach at Choicepoint, this led to USD 10 million in nalties for security breaches and USD 5 million in redress to rs (FTC, 2006).

e recently we have seen what will undoubtedly be a landmark case, rity breach at the US retailer T.J. Maxx in December 2006. Many are suing the retailer for damages following this breach. Among them banks that had to reimburse their customers for fraudulent ions stemming from credit card information that was stolen at T.J. Recently, the retailer has reported that the breach has already cost it 35 million – and the case is far from over. A security company

Sarbanes-Oxley, the Health Insurance Portability and Accountability the Gramm Leach Bliley Act While there is disagreement over the eness of these laws, issues of liability and compliance have shown to rs for increased security efforts (*e.g.* Ernst & Young, 2007; Lords, 152)

er countries have different regulatory regimes in place However, e parallels Data protection laws could potentially have similar So far, however, these effects, if they are indeed occurring, are less visible Predictably, the debate is shifting towards the issue of to connect sanctions to these liabilities The UK Information ssioner recently called for criminal sanctions "for those who ly and recklessly flout data protection principles" (Shifrin, 2007)

ry of end-user incentives

users have been the focus of considerable debate regarding Internet As has been reported before, many externalities emanate from end ecurity decisions – or non-decisions Interestingly, both for home d large users, there exist incentives that are potentially very strong – he risk of significant damage to themselves resulting directly from cisions

problem is, however, that their risk perceptions are often not nt with the technological realities in which they operate To the hat end users do appreciate the risks they face, there are significant s when they attempt to act on that information For home users, tools are often too complex and partially effective at best For large nd private organisations, the situation is remarkably similar While en have more expertise available, the security challenges are also ially more complex in light of the complicated array of systems, and the organisational arrangements around them

a result, end users generate externalities, the costs of which are es passed back to them But in many cases, the costs are passed on, rnalised by, other market players, which consider them part of the doing business in the information industry, or the costs are absorbed ty at large

Annex 5.A1. List of Interviewees

007, 41 in-depth interviews were conducted with 57 professionals
ganisations participating in networked computer environments that
ronted with malware. Below is a full list of those responding.

each instance, the following questions were asked: how the
ation was confronted with malware, what its responses were, what
fs were associated with these responses, and how the organisation
cted by the actions of other market participants.

details on the research design and its scope and limitations, please
ex B: Research Design for Economics of Malware.

Joseph	Oracle [US]
uzana	Telstra BigPond [AUS]
Michael	PayPal [US]
remy	Confederation of British Industry [UK]
rf Brian	Mozilla Foundation [US]
ns Arno	St. Elisabeth hospital [NL]
en	Go Daddy [US]
Hans	St. Elisabeth hospital [NL]
Mary Ann	Oracle [US]
oen	Consumentenbond (Consumers Union) [NL]
Eric	France Telecom / Orange [FR]
ert	ABN AMRO [NL]
John	StreamShield [UK]
Wim	FI-ISAC / Rabobank [NL]
Jaap	KPN [NL]
mon	XS4All [NL]
teve	Microsoft [US]
n	Comcast [US]
teve	Telstra BigPond [AUS]
Paul	ServePath [US]
ouwe	GOVCERT [NL]
er	Oracle [US]
Scott	XS4All [NL]

Graeme	Symantec [UK]
Dave	Fellow to the ICANN SSAC [US]
Niels	Google [US]
na Richard	Federal Trade Commission [US]
oss	Tucows [CA]
r. Thomas	BSI (Federal Office for Information Security) [DE]
ve	TrendMicro [JP]
ns	Queen Mary University of London [UK]
Roeland	GOVCERT [NL]
Jerry	KPN [NL]
Daniel	Federal Trade Commission [US]
Michael	NVB (Dutch Association of Banks) [NL]
Werner	BSI (Federal Office for Information Security) [DE]
Kevin	ACDNet [US]
an Jacques	Surfnet CERT [NL]
Louis	Federal Trade Commission [US]
n	Shell International [NL]
Nick	BT [UK]
en Frits	ABN AMRO [NL]
Heide Martijn	KPN-CERT [NL]
Franck	France Telecom / Orange [FR]
nthony	Shell International [NL]
remy	Symantec [UK]
Rick	Support Intelligence / Alice s registry [US]
Colin	APACS [UK]
Rich	Michigan State University [US]
Jeff	Microsoft [US]
k Bill	Packet Cleanng House [US]

er 6. The Market Consequences of Cybersecurity: ining Externalities and Ways to Address Them

preceding chapter reported on the efforts and incentives of a variety net market participants. It indicated a number of market-based e mechanisms that contribute to enhanced security but also other s in which decentralised actions may lead to sub-optimal outcomes sing question is: Are participants in the information and nication markets responding adequately to malware, or are ments possible? Pointing to a variety of reports that show increases cious attack trends, one might conclude that markets are not ing adequately. Our analysis revealed a more nuanced picture.

r categories of externalities

l-world markets rarely meet the preconditions of standard economic For example, decision makers rarely have complete information, erate under conditions of bounded rationality, and they behave nistically. For these reasons, individual decisions rarely are as ideal ibed by abstract models. Rather, real-world decisions are a process ddling through" second and third-best solutions, especially in an ment of rapid technological change. Whether a decision was good or ften revealed only after-the-fact.

essing the direct and indirect economic cost of malware in real- onditions is hence an important aspect of designing countermeasures. ie provision of security entails cost, tolerating a certain level of ty is economically rational. Therefore, the level of security realised on the costs and benefits of security to individual actors, and on l collective measures to enhance security. Two key questions are

osts are externalised (passed on) to other market players or society at e, how serious are they in relation to the internalised (absorbed) s?

le keeping in mind the scope and limitations of our study, we can number of tentative conclusions with regard to these questions the information market's value net, three relevant situations emerge market participants.

ry 1: No externalities; market participants absorb all the f their security decisions.

decision-making unit, be it an individual user or an organisation, y assesses security risks, bears all the costs of protecting against threats (including those associated with these risks) and adopts iate countermeasures. The private and societal costs and benefits of decisions are aligned. There may still be significant damage caused ware, but this damage is borne by the market player itself. This would be economically efficient, but due to the high degree of endency in the Internet, it is rare.

t does not mean these situations are non-existent. In principle, end be they large organisations or skilled home users – who take e security measures and successfully prevent their machines from ompromised generate no externalities for the rest of the market– some experts might argue that under certain conditions such ur creates positive externalities that are not taken into account and d to an sub-optimal level of private investment (Kunreuther and 003).

eral interviewees in our field survey claimed that in recent years, ve not had any malware infection within their organisation's . We were not in a position to check the validity of these claims, but t unreasonable to assume that there are cases where malware is ully fought off, or where the effects of malware infections are, by e, limited to the owner of the infected system.

ry 2: Externalities are created, but they are borne by agents n manage them.

l on others into account But they can also result from a lack of skills with security risks, or financial constraints faced by an individual or ation.

ong as somebody else in the market internalises these costs, and this in a position to influence these costs – *i.e.* it can influence the trade-offs of the agents generating the externality – then the security hieved by the whole value net may deviate less from a social n than without such internalisation. This scenario depicts a relatively case and numerous examples were found that confirm externalities ing internalised by other market players

P example

s have started to manage the security problems generated by their rs – *e.g.* by quarantining the infected machines of end users. As ey absorb some of the costs generated by the sub-optimally low ent in security by their own customers. ISPs internalise these costs, not doing would lead to even higher costs being imposed on them, may experience blacklisting, rising customer support and abuse ment costs and possible reputation effects.

key point here is that ISPs are internalising these costs, but that they in a position to influence the behaviour of the agents generating the ity – *i.e.* their own customers. For example, if they increasingly blacklisting because of spam from infected end-user machines their network, one of the options they have is to block port 25. That significantly reduce the degree of blacklisting and the costs ed with it. Of course, such a measure also has costs and implies a f with other objectives, such as the kind of services the ISP can offer omers. They may opt against blocking port 25 for a variety of That does not mean, however, that the externality is not a given, but y can actually influence its magnitude. This is different from, say, an erce company who has to buy DDoS (mitigation services from its ause of botnet attacks. That company cannot do anything about and thus the costs to defend itself against them is simply considered f doing business.

only internalise a part – some experts would say a minor part – of rnalities caused by their customers. For example, while ISPs are

e of online financial services

ther instance of this type of externality was found in the case of l services The incentives of financial service providers are such that cases they compensate customers for the damage they suffer from raud In that sense, they internalise the consequences of sub-optimal investments by their customers, as well as the software vendors oftware is exploited to execute the attacks Many financial service s claim they compensate all malware-related losses If that claim is , then the security level achieved by the whole value net may not be from the optimum The financial institutions bear the externalities, are also in a position to manage the risk through security measures pose on online financial services

vever, there are three important considerations to take into account

unclear what the reality is of customer compensation under the ent liability regime Some researchers suggest that many claims are act refused and that not all of the victim's damage is compensated, the direct loss (Schneier, 2005; Anderson, 2007)

re is debate within the industry to change the banking codes so as to gn more liability to the customer New Zealand has already adopted vised code to this effect That would change the incentives which ht push the level and focus of security investments of the financial tutions away from the social optimum (Anderson, 2007)

n if customer damage is compensated, one could argue that there are externalities in the sense that important social efficiencies could be ed if people had higher trust in these services and could adopt them e quickly. These benefits would outweigh the additional security stments that would be needed While the magnitude of these rnalities is unknown, the financial service providers are the ones stand to gain most from maintaining high trust in the e-channel In r words, this is a problem of incomplete information, rather than of ligned incentives

ry 3: Externalities are borne fully by other market pants or by society at large.

individual unit may correctly assess the security risks given its

ike in Category 2, no other agents in the information and nication value net absorb the cost. Or, if they do, they are not in a to influence these costs – i.e. influence the security trade-offs of the generating the externality. Hence, costs are generated for the whole nd society at large. These are the costs of illegal activity or crime ed with malware, the costs of restitution of crime victims, the cost of orcement associated with these activities, and so forth.

hermore, the externalities may take on the more indirect form of growth of e-commerce and other activities. Slower growth may entail icant opportunity cost for society at large, if the delayed activities have contributed to economic efficiency gains and accelerated . A comprehensive assessment of these additional costs will demand rted effort but will be necessary to determine the optimal level of o fight malware.

e of lax security by end users

most poignant cases in this category are the externalities caused by security practices of end users. Some of these externalities are sed by other market players, but many are borne by the sector as a nd society at large. These externalities are typically explained by the of incentives for end users to secure their machines.

ould be more precise, however, to argue that the end users do not any incentives to secure their machines. While malware writers rposefully chosen to minimise their impact on the infected host and t their attacks at other targets, there is also a plethora of malware loes in fact attack the infected host – most notably to scour any l information that can be used for financial gain. In that sense, end o have a strong incentive to secure their machines. Unsecured s cannot differentiate between malware that does, or does not, affect er of the machine. If the machine is not sufficiently secured, then to assume that all forms of malware can be present. The fact that entive is not perceived by the end user is an issue of incomplete tion rather than a lack of incentives.

al and efficiency effects

en externalities are borne by agents who can manage them (Category are usually *distributional* in nature. That is, there is a mere shifting osts (and benefits) between the actors involved. In the case of ISPs, rs shift to ISPs most of the cost of secure online connections, but the in a position to manage those costs via various actions.

ontrast, overall *efficiency* externalities materialise if the cost of g a given level of information security can be reduced for all the ants in the sector. This differentiation is also important in the on of alternative strategies for coping with problems of malware. easures, such as a modification of liability rules, may predominantly burden of combating malware from one set of actors to another. In ases, it will be critical that the resulting attribution of costs and is better aligned with the true cost structure of the value net. Only in will efficiency be improved.

to the high degree of interrelatedness, nearly all the three ble categories of externalities discussed in the previous section are with both types of effects. In general terms, however, we would hat Category 2 externalities have mainly distributional effects, while y 3 will have distributional, as well as efficiency effects. From a perspective, the latter is obviously a more damaging form of market In the case of Category 2, efficiency effects are not a given – *i.e.* ses need not imply a suboptimal level of security for the value net as Banks, for example, internalise the security-related externalities ed by end users and others. This does not need to have efficiency because the banks can mitigate the risks of end users and thus can f the damage against the costs of mitigation. In fact, it may have a effect on efficiency, if the banks can manage the risks better than users themselves.

important to keep in mind that many malware-related externalities ts have their origin in illegal and criminal behaviour. Illegitimate players imposing costs on others. In that sense, the oft-cited analogy nalities in environmental pollution does not hold. In the example of n, there is a market player that benefits from the production process that pollution. In that case, the guiding principle of standard ic theory is to internalise the costs of pollution so that the agent he level of production to be more in line with the social optimum.

nd not by individual stakeholders This is currently happening, for , in the area of law enforcement, but it is not clear whether it is at an level

lts on the costs of malware

ough the malware-related costs of security measures are considered ary, estimates provided by players range from 6-10% of the ent in ICT No clear estimates of the effects of malware on operating s were available, although we did find that most organisations did ace such effects There was evidence throughout the empirical of concern that such effects are important, although no specific on as to their magnitude is available The concern with this broader externality seems to motivate several players, especially in es sensitive to reputation issues, to increase investment in security dd a "safety margin" when deciding on levels of security.[1]

information collected in this research project from actors across the tion and communication value net allows the conclusion that the rivate and public costs of prevention are substantial With few ons, many actors have had to increase their security-related ents as a response to the higher benefits of security associated with es of transactions conducted via the Internet and the increasing of attacks

wever, each actor typically only acts based on the perceived es In literally all cases, there were important costs and benefits that at other stages of the value net and were hence outside the decision- process Our research showed that due to feedback effects inherent et co-ordination, the magnitude of these externalities is probably than hitherto assumed On the other hand many of these externalities uncorrected leaving the system overall in a sub-optimal state

collective costs of fighting malware, ranging from the costs of ing public-private organisations such as CERTs or CSIRTs, to the public education campaigns and law enforcement, add to these costs Finally, all actors pointed to the potentially high indirect costs are in the form of slower migration to efficiency-enhancing forms of ic transactions Taken together, the direct and indirect costs of

s

ough the research in this report was not designed to develop specific ecommendations, some general concluding remarks are nonetheless [2] With regard to the interrelationships within the information and nications-related activities, it seems that the incentives of many of mercial stakeholders are reasonably aligned with minimizing the of externalities on the sector as a whole

incentives typically have the correct directionality But in a variety they are too weak to prevent significant externalities It is important however, that all market players we studied experience at least some ences of their security trade-offs on others In other words, there edback loop that brought some of the costs imposed on others back gent that caused them

found many such feedback loops, which mitigate the externalities from less-than-optimal security decisions All market players we experience such feedback, which potentially brings their security fs closer in line with that of society in general We also noted, r, that in many cases these feedback loops are too weak or too d to effectively change the security trade-offs that caused the ities to emerge in the first place

erms of policy development, a key strategy would be to strengthen ing feedback loops and create new ones where possible That would p public policy out of the realm of having to decide how secure is nough when it comes to defending against malware

en the complexity of the interrelationships, there are no panaceas ld address all the issues in one sweep From our analysis, we e that measures that increase the costs of malware perpetrators will, r things being equal, help reduce the overall cost of security But arket participants may then be induced to reduce their investments in , the damages associated with security breaches may not decline

larly, measures that increase the level of security may increase related costs without actually lowering the damages related to breaches In a highly interrelated system, it is often difficult to the overall impact of a policy measure due to feedback and pated effects It is therefore necessary to search for measures that are

Notes

or a literature review of the available estimates of the costs of malware d network security in general, see Bauer, J M , M J G Van Eeten and Chattopadhyay (Forthcoming). *Financial Aspects of Network Security alware and Spam* ITU (International Telecommunication Union), *ww itu.int/ITU-D/cyb/*

or those readers interested in policy recommendations, note the recent udy, Anderson, R., *et al.* (2008), 'Security Economics and the Internal arket', European Network and Information Security Agency, *ww enisa europa eu/doc/pdf/report_sec_econ_&_int_mark_2008 131 pdf*

Part III. Malware: What Can Be Done?

ould agree that the damage caused by malware is significant and be reduced, even though its economic and social impacts may be quantify. That said, Part III of this book focuses on the factors that e considered in assessing what action to take, and by whom, against . These include the roles and responsibilities of the various market ants[1], and the incentives under which they operate (Chapter 7); the s already being undertaken by communities more specifically l in fighting malware (Chapter 8), and finally an assessment of what uld be taken to create a holistic and comprehensive approach to (Chapter 9)

ording to the 2002 *OECD Guidelines for the Security of Information*

7. The Role of End Users, Business and Government

ware affects individuals, business and government in different ways se participants can play a role in preventing, detecting, and ing to malware with varying levels of competence, resource, roles ponsibilities, as called for in the *OECD Guidelines for the Security of tion Systems and Networks: Towards a Culture of Security* (the Security Guidelines") Better understanding the roles and bilities of the various participants in relation to malware is nt to assessing how to enhance the fight against malware.

pants

ong the various participants, those concerned by malware are.

End users (home users, small and medium-sized enterprises (SMEs), public and private sector organisations) whose data and information systems are potential targets and which have different levels of competence to protect them.

Software vendors, which have a role in developing trustworthy, reliable, safe and secure software.

Anti-virus vendors, which have a role in providing security solutions to users (such as updating anti-virus software with the latest information on malware).

Internet Service Providers (ISPs), which have a role in managing the networks to which the aforementioned groups connect for access to the Internet.

Domain name registrars and regulators, which determine if a domain is allowed to be registered and potentially have the power to

example, in detecting, responding to and recovering from security incidents and issuing security bulletins about the latest computer network threats or vulnerabilities associated with malware attacks, or in co-ordinating nationally and internationally the resolution of computer network attacks affecting its constituency or emanating from its constituency.

Law enforcement entities, which have a mandate to investigate and prosecute cybercrime.

Government agencies, which have a role to manage risks to the security of government information systems and the critical information infrastructure.

Governments and inter-governmental organisations, which have a role in developing national and international policies and legal instruments to enhance prevention, detection and response to malware proliferation and its related crimes.

nd disincentives – Highlights from Part II

er comprehension of how market players are, or are not, incentivised important to understand how they are responding to malware and assess how to enhance the fight against malware. Incentives are by the costs and benefits associated with the possible responses of rket player. In some cases, there may be strong incentives for a player to develop policy and technical approaches to more ely combating malware. In other cases, incentives may be less or even non-existent. Actors make their own trade-offs regarding nd of security measures they deem appropriate and rational, given siness model.

y limited information as to how individual actors actually make their tion security decisions is available in the public domain, which t difficult to calibrate any form of public policy. Economic decisions gard to information security depend on the particular incentives d by each market player (Eeten and Bauer, 2008).

Box 7.1 Different types of incentives

ntives are often classified as being either monetary (financial, rative) or non-monetary (non-financial, moral)

ncial incentives typically connect degrees of achievement of an objective onetary payments They include factors such as tying the salary of an ee to corporate performance, the ability to make a super-normal profit by g a risky innovation, or the bottom line effects of potential damage to a eputation

-financial incentives work through self-esteem (or guilt) and community tion (or condemnation) They encompass norms and values, typically with peers, and which result in a common understanding as to the right of action, or the set of possible actions that should be avoided in a ar situation

se incentives are rooted in economic, legal, and other mechanisms, g the specific economic conditions of the market, the endence with other players, formal legal rules as well as informal Ideally, the relevant incentives should assure that private costs and of security decisions match the social costs and benefits Any policy to combat malware, therefore, needs to take into account the incentive mechanisms and examine whether they could potentially fied to produce more efficient outcomes at the societal level

llustrate, an online financial service provider might decide that it is st-effective to compensate the damage of customers victimised by e, rather than to introduce new security technology reducing this Not only may those technologies be more costly than the actual amage, they could raise the barriers for customers adopting these The incentives under which these service providers operate may economically rational to keep the damage of malware at manageable ather than to push it back further

he societal level, the key policy question is whether the decisions of ke into account the costs and benefits that result from their response are There are instances where the incentives of actors do not reflect s their decisions impose on others – *i e* these costs are externalised.

alities related to malware

l-world markets rarely meet the preconditions that are assumed to ording to standard economic theory For example, decision makers ave complete information, they operate under conditions of bounded ty and behave opportunistically. For these reasons, real-world al decisions are often a process of "muddling through" second and st solutions, especially in an environment of rapid technological Moreover, many malware-related externalities and costs have their n the illegal or criminal behaviour of illegitimate players imposing legitimate market participants.

essing the direct and indirect economic costs of malware and g countermeasures is an important issue As the provision of entails cost, tolerating a certain level of insecurity is economically The resulting level of security is dependent on the costs and of security Relevant questions that need to be addressed include

Are market players taking the full range of costs into account when making security decisions?

What costs are externalised to other market participants or society at large?

lings regarding incentives and externalities for the different market ants confronted with malware reveal three situations no ities; externalities that are borne by agents that can manage them; ernalities that are borne by agents who cannot manage them or by at large (Eeten and Bauer, 2008). For a detailed discussion of these tegories, see Part II of this report.

ve structures for market participants

research project presented in Part II of this report[1], conducted to understand current incentive structures and possible externalities, hat the overall response to malware emerges from the interaction of ket participants and the degree of compatibility (or incompatibility) respective incentive structures

ems that the incentives of many of the commercial stakeholders are

ack to the agent that caused them – even if in some cases the force edback loop has so far been too weak or too localised to bring their ur in line with the societal optimum.

some participants, an important mechanism to achieve this nate result is the interdependence between them. In other instances utation effects that align incentives with the socially optimal choice. ects may operate independently or jointly, as in the case of ISPs.

instance, a user with insufficient malware protection may cause an ity whose cost is, in part, borne by the service provider, in part by Ps, and in part by society at large (*e.g.* costs of law enforcement, reduced trust in e-commerce). An ISP may incur costs to enable its to isolate single users that might spread malware due to insufficient on of that user's machine. Part of this externality is thus internalised SP because of the incentives of the provider to protect the integrity rvices and to avoid blacklisting and the negative effects this might r its operating costs, its reputation and consequently its revenues and prospects.

on society at large

ong other findings, the research in Part II also shows that whereas ternal effects are internalised at the level of the whole information y ecosystem, there are some effects that need to be considered as ities to society at large.

example, malware and its effects may tarnish the reputation of es that rely heavily on electronic transactions, such as banking or e. If electronic platforms are used less frequently than would se be the case, then the forgone efficiency improvements can be ed an externality cost to society of malware. Moreover, malware mish trust in the working and security of e-commerce overall. f this results in slower diffusion and growth, one could consider the ed potential efficiency gains as a cost to society. Such potential uld occur at the sector level but they could also manifest themselves r overall economic growth rates. There is evidence throughout the f concern that such effects are important, although no specific on as to their magnitude is available.

urity problems and the related economic costs to society may have
s:

y are the outcome of relentless attacks on the information and
munication infrastructure by criminals, and

en an overall external threat level, they may be aggravated by
repancies between private and social costs and benefits which are
outcome of decentralised decision-making in a highly interrelated
system

ors in both the criminal world and within the information and
nications system respond to the economic incentives they face For
ket players assessed in the empirical study presented in Part II, a
ncentive structure exists which includes positive incentives as well
centives to take action against malware

Note

he research in Part II of this report is based on in-depth interviews in
ve countries with representatives of market participants, including
ternet Service Providers (ISPs), e-commerce companies with a focus on
line financial services, software vendors, hardware vendors, registrars
d end users – complemented by interviews with regulators, CSIRTs,
ANN, security services providers and researchers

Chapter 8. What Is Already Being Done?

er understanding of the nature, successes and limitations of ongoing
y communities more specifically involved in fighting malware is
portant to assessing how to enhance prevention of, and response to,

key efforts

stantial efforts by various participants have been made within OECD
s and APEC economies and at the international level to raise
ss, measure malware, develop or amend legal frameworks,
en law enforcement, and improve response. For example:

Many websites and resources exist to help end users and SMEs secure their information systems.

Many entities track, measure and sometimes even publish data on their experience with malware and related threats.[1] Furthermore, schemas[2] exist to provide single, common identifiers to new virus threats and to the most prevalent virus threats in the wild to reduce public confusion during malware incidents.

Several informal networks have been created that are a key element of the response community's ability to respond to incidents resulting from malware. CERT/CC has catalogued 38 national CSIRT teams, 19 of which are in OECD countries, and 16 of which are in APEC economies (CERT Coordination Center, 2006). In addition, they hold annual meetings for national CSIRT teams to gather and share information about numerous issues, including malware.

Numerous countries across the world have legal provisions against

online and 43 countries across the globe are now party to the Convention.

Law enforcement agencies and organisations across the world have made important efforts to find malicious actors and bring them to justice for the crimes they commit. The law enforcement community has created points of contact networks and other similar schema to help cross-border co-operation in recognition that the majority of these crimes cross legal and jurisdictional boundaries. Law enforcement agencies and business typically use tools which implement the Whois protocol to query database servers operated by the domain name registrars and Regional Internet Registries for data on domain name owners, Internet Protocol address and Autonomous System Number allocations that can identify the asserted physical locations where unlawful activity is taking place, and the relevant service providers (ISPs), which, in turn, can provide information regarding their customers.

ISPs are operating in highly competitive markets and are taking proactive steps in the fight against malware, such as quarantining infected machines.

Software vendors have increased efforts to improve the security of their software. The deployment of vulnerability patches has improved. Arguably more important, many software vendors put software development processes in place that are increasingly aware of and focusing on security issues.

Governments across OECD countries and APEC economies are taking policy, legislative and technical measures to address malware[3]. In particular, they are working, in co-operation with the private sector, to protect their government critical information infrastructure from electronic attack.

se communities have made significant efforts to address the issue of
and anecdotal evidence suggests a much greater awareness of the
than only a few years ago. The nature of malicious and criminal
activity, however, is such that these communities are always
g up" with the malicious activities. This report has shown that
ing all malware is neither feasible nor economically rational but
it harder for malicious actors to succeed – through prevention and

, structures and initiatives that address malware

s following section provides examples (rather than a comprehensive existing instruments, structures and initiatives, at the national and onal levels, whose purpose is to help address the issue of malware

ness raising

areness is an important line of defense against malware and the esulting from its use. Both the public and private sectors, separately artnership, have taken initiatives to educate Internet users about

ia - E-Security National Agenda (ESNA)

Australian Government established the ESNA in 2001 to create a nd trusted electronic operating environment for both the public and sectors. A review of the ENSA in 2006 found that the online ment is highly interconnected and that e-security threats to different s of the Australian economy can no longer be addressed in isolation context, the Australian Government announced AUS$73.6 million ur years for new measures to strengthen the electronic operating ment for business, home users and government agencies.[4] In , the Australian government is undertaking the following initiatives:

An annual National E-Security Awareness Week will be held in collaboration with industry and community organisations. The week encourages Australian home users and SMEs to undertake smart behaviour online. A pilot Awareness Week was held in October 2006.

The enhancement of the Government's e-security website *www.staysmartonline.gov.au* is the key mechanism to disseminate simple e-security information and advice to home users and small businesses on how they can secure their computers and adopt smart online practices.

The development of an e-security education module for Australian schools to focus on raising e-security awareness of young Australians.

Australian Government has also developed a number of booklets to
ge Australian consumers and small businesses to protect themselves
e-security threats.[5]

ia Netalert[6]

nched in August 2007 by the Australian government, Netalert is an
safety initiative that combines an Internet safety information
n, a National Filter Scheme to provide free access to an Internet
filter to help block unwanted content, and a website and hotline to
advice about protecting children online, as well as access to the free
nd information about how they work.

ia Stay Smart Online website

Stay Smart Online website provides simple step by step advice to
sers and small and medium sized-enterprises (SMEs) on how they
ect themselves on line.

er Internet Plus Programme[7]

he EU level, the Safer Internet plus programme promotes safer use
ternet and new online technologies, particularly for children, as part
erent approach by the European Union.

e Online[8]

Get Safe Online (GSO) is the UK Government website that aims to
awareness raising information about safe online practices for home
E Internet users. The website complements the ITsafe website and
on awareness raising activities with links to popular websites. The
n material provides information on e-mail, malware, phishing and
. The website was initiated by a joint agreement between the UK
ment and the private sector, namely sponsors from technology, retail
nce.

Safe Online Week (GSOW) was launched in October 2006 and
l various awareness raising activities. Activities of the Week
l an Internet safety summit with an objective to initiate liaison
government, industry and the public sector with a focus on issues
et crime. A Memorandum of Understanding (MOU) was signed that

service is funded by the UK Government Home Office and uses
tion provided by the Centre for the Protection of National
ucture (CPNI). This Government department provides electronic
for the UK Government. The aim of the ITsafe website is to advise
est methods necessary to protect personal and business data. ITsafe
ged by a Government team on behalf of the CPNI by the Central
for Information Assurance (CSIA).

aland Netsafe[9]

safe is a partnership between The Internet Safety Group (ISG), an
dent non-profit organisation responsible for cybersafety education in
ealand, and the New Zealand Ministry of Education with
tation and sponsorship from industry, police, banking and others.
us of NetSafe is to provide children with information about sexual
r similar instances of abuse online. The site also has information
nalware, computer maintenance, peer 2 peer file sharing, IRC
risks, hackers and other e-security information is provided.

NetSafe website covers topics including online safety for children
nagers, online security for businesses, Internet fraud and law
ment, online gambling, copyright, e-commerce and the law. NetSafe
ts a cartoon website, Hector's World, designed to entertain and
children about online safety.

Kingdom ITsafe[10]

ITsafe initiative is a UK website that provides simple and easy to
nd e-security alerts and threats to both home and small business
users. Advice and information contained within the website is free
udes varying types of e-security threat alerts and warnings enabling
lectronic environment for Internet users.

States Onguard Online[11]

GuardOnline.gov is a website maintained by the US Federal Trade
ssion and partners such as the US Postal Inspection Service, the US
ment of HomeLand Security, the US Department of Commerce, and
rities and Exchange Commission to provide practical tips from the

ted States StaySafeOnline[12]

ySafeOnline is a website provided for the public by the National Security Alliance, a US industry coalition supported by the US ient of Homeland Security to provide cyber security awareness to he user, small businesses, higher education, and K-12 students. It free and non-technical cyber security and safety resources g alerts, tips, and reports to the public so consumers, small ses and educators have the knowhow to avoid cyber crime.

States – National Awareness Month

United States Government in collaboration with industry holds an National Cyber Security Awareness Month (NCSAM). The month raise awareness about online security and how to adopt safe online s. The activities and events held in the month focus on home Internet MEs, government, education and the corporate sector.

gels[13]

nangels is a US based group of 13-18 year-old volunteers who have ecially trained by the local law enforcement, and many other leading xperts in all aspects of online safety, privacy, and security including . After completion of the required training, the Teenangels run programs in schools to spread the word about responsible and safe to other teens and younger children, parents, and teachers.

ations

l of Europe Convention on Cybercrime

Convention of the Council of Europe (COE) on Cybercrime is the d only legally binding multilateral treaty addressing the problems by the spread of criminal activity on line. Signed in Budapest, y in 2001, the Convention entered into force on 1 July 2004. sing digitalisation, convergence and continuing globalisation of r networks, the Convention requires its signatories to establish laws riminalise security breaches resulting from hacking, illegal data tion, and system interferences that compromise network integrity dability.

g international co-operation." To achieve these goals, the signatories to establish certain substantive offences in their laws which apply to er crime. Although malware is not *per se* mentioned in the tion among the illegal activities that signatories must criminalise, it ectly covered under closely related listed crimes including illegal o information systems, computer data, and computer-related fraud [14]

Convention encourages a more coherent approach in the fight cyber attacks. It also includes provisions for a 24 hours per day, 7 r week online crime-fighting network and facilitates public-private hips. The Convention also provides extradition and mutual legal ce treaties' provisions between signatories where none exist.

date, the Convention has been ratified by 21 countries and signed by tional countries (Council of Europe, 2001). Some companies in the ector have taken some initiatives to help ensure a larger impact of vention's principles [15]

on and response

ny countries have a watch, warning and incident response function in n of a CSIRTs or CERT. It is important to recognise that not all and CERTs are alike. Some are public entities residing in the ment structure, some are publicly and privately funded entities with mandates and still others are associated with academic ons [16] It is widely accepted good practice that governments develop nt a CSIRT or CERT with national responsibility [17]

some cases, entities within a country are required to report tion security incidents to a central government authority competent e them. In some cases this entity is a CSIRT/CERT. For example, in it is obligatory that significant violations of information security, nd disturbances in public telecommunications be reported to the CSIRT of Finland, CERT-FI [18] One example of a "significant " is considered activation of malware in telecommunication service s' own systems". In order to fulfil this regulation for external reporting, the telecommunications service provider must have e internal processes for detection and reporting of as well as y from information security incidents and threats. This model has ccessful in Finland because the government has proven to the

he United States, all civilian government agencies are required to nformation security incidents to US-CERT.[19] In both Finland and the States a standard incident report form is provided

tional initiatives

of Incident Response Security Teams (FIRST)

ST brings together a variety of computer security incident response (CSIRTs) from government, commercial, and educational tions in 37 countries. FIRST aims to foster co-operation and co-on in incident prevention, to stimulate rapid reaction to incidents, romote information sharing among members and the community at Membership in FIRST enables incident response teams to reach arts in other countries that can help them to more effectively to security incidents

cific CERT (APCERT)[21]

CERT is a contact network of computer security experts in the Asia region established to improve the region's awareness and ncy in relation to computer security incidents. APCERT works to co-operation on information security, facilitate information sharing nology exchange and promote collaborative research on subjects of to its members. APCERT also works co-operatively to address legal elated to information security and emergency response across boundaries.

ean Telecommunication Union

Caribbean Telecommunications Union (CTU) has been involved in lopment of an Internet Governance Framework for the Caribbean on of the Caribbean Community (CARICOM). The CTU has held ignificant Internet Governance forums at which delegates raised the establishing a Caribbean Computer Emergency Resource Team for timely detection of security incidents in regional computer s, their proper handling and post-detection activities. There is now a body of ICT practitioners who have expressed the need for a CERT tablished for the Caribbean. In response, the CTU will be engaging

ropean Government CERT Group (EGC)

EGC[22] group is an informal group of governmental CSIRTs that is ing effective co-operation on incident response matters between its s, building upon the similarity in constituencies and problem sets governmental CSIRTs in Europe. To achieve this goal, the EGC s jointly develop measures to deal with large-scale or regional security incidents, facilitate information sharing and technology e relating to IT security incidents and malicious code threats and bilities, share knowledge and expertise, identify areas of ative research and development on subjects of mutual interest, and ge formation of government CSIRTs in European countries

ordination Council CERT (GCC CERT)

C CERT aims to supervise the establishment of national response n Saudi Arabia, the United Arab Emirates, Qatar, Bahrain, Kuwait an

orce CSIRT (TF CSIRT)[23]

activities of TF CSIRT are focused on Europe and neighbouring s, in compliance with the Terms of Reference approved by the A Technical Committee on 15 September 2004. TF CSIRT provides for the European CSIRTs to communicate, exchange experiences wledge, establish pilot services, and assist the establishment of new Other goals of the TF CSIRT include:

To promote common standards and procedures for responding to security incidents.

To assist the establishment of new CSIRTs and the training of CSIRTs staff

ement

ic structures

ler EU legislation the provisions detailed on the next page may be d by administrative bodies and/or criminal law authorities. Where

ogether the technical and investigative skills of different agencies
ation protocols are needed to cover such areas as exchange of
tion and intelligence, contact details, assistance, and transfer of

he United States, both the Federal Bureau of Investigation and the
ecret Service have authority to investigate malware crimes in
1 of the Computer Fraud and Abuse Act (Title 18, United States
ection 1030). Violations of the Computer Fraud and Abuse Act are
ted in US federal courts by the US Department of Justice, through its
orney's Offices and the Criminal Division's Computer Crime and
ual Property Section. The US Department of Justice also prosecutes
-related crimes such as criminal violations of the CAN-SPAM Act
8, United States Code, Section 1037), access device fraud (Title 18,
States Code, Section 1029) and Aggravated Identity Theft (Title 18,
States Code, Section 1028A).

tional mechanisms

ious international forums focusing on security, privacy or consumer
on issues, devote substantive efforts to tackle the multifaceted nature
crime.

ntact Network of Spam Authorities (CNSA)[24]

the initiative of the European Commission, an informal group was
consisting of National Authorities involved with the enforcement of
13 of the Privacy and Electronic Communication Directive
/EC called the Contact Network of Spam Authorities (CNSA). In
SA, information on current practices to fight spam is exchanged
National Authorities, including best practices for receiving and
g Complaint information and Intelligence and investigating and
ng spam. The CNSA has set up a co-operation procedure that aims
tate the transmission of complaint information or other relevant
nce between national authorities. The CNSA has drawn up a co-
n procedure to facilitate cross-border handling of spam complaints
orking on the issue of spyware and malware.

ncludes almost 50 countries, was created among the G8 countries in
address the unique challenges that high-tech crime investigations
law enforcement. The 24/7 Network is designed to supplement (but
ace) traditional mutual legal assistance frameworks by providing a
ism to facilitate the preservation of electronic evidence. The 24/7
k has been instrumental in preserving evidence in hacking, fraud, and
crime investigation and for providing training on topics such as

l

rpol[25] is an international police organisation with a mission to
or combat international crime. Interpol has decentralised its
me expert teams around the world through the establishment of
Working Parties on Information Technology Crime for Europe,
America, Asia, South Pacific, and Africa.[26] Interpol's European
g Party on Information Technology Crime (EWPITC) has for
compiled a best practice guide for experienced investigators from
orcement agencies.[27] It has also set up a rapid information exchange
under an international 24-hour response scheme, listing responsible
within more than 100 countries. This scheme was notably endorsed
G8 24/7 HTCN

Action Plan (LAP)[28]

purpose of the London Action Plan is to promote international spam
ment co-operation and address spam-related problems, such as
raud and deception, phishing, and dissemination of viruses. The LAP
participation from government, public agencies, and the private
om over 27 countries.

tional Consumer Protection Enforcement Network (ICPEN)

International Consumer Protection and Enforcement Network
) is a network of governmental organisations involved in the
ment of fair trade practice laws and other consumer protection
s. ICPEN was founded in 1992 by 20 countries and in co-operation
OECD and the EU; the network now has 29 participant countries. A

ers face in conducting cross-border transactions for goods and
ICPEN co-operation does not include the regulation of financial
and product safety and it does not provide a platform for the
ment of specific redress for individual consumers.

EN has established several working groups including: The Mass
ng Fraud Working Group, Best Practices Working Group,
atch Working Group that covers some of the issues associated with
. In addition, their Internet Sweep initiative seeks to find and
e fraudulent and deceptive Internet sites.

tion

le malware is rarely mentioned as such in legislation, malicious
s that use malware are often covered by numerous existing areas of
uding criminal law, consumer protection law, data protection law,
munication law, and anti-spam law. A survey by the OECD Task
n Spam at the end of 2004 indicated that most OECD countries have,
ast few years, set up a legislative framework in order to fight spam
y apply to malware in some cases.

he European Union, under the e-Privacy Directive and the General
otection Directive, national authorities have the power to act against
owing illegal practices:

Sending unsolicited communications (spam) [29]

Unlawful access to terminal equipment; either to store information – such as adware and spyware programs – or to access information stored on that equipment [30]

Infecting terminal equipment by inserting malware such as worms and viruses and turning PCs into botnets or usage for other purposes [31]

Misleading users into giving away sensitive information such as passwords and credit card details by so-called phishing messages [32]
Some of these practices also fall under criminal law, including the Framework Decision on attacks against information systems [33]. According to the latter, Member States have to provide for a maximum penalty of at least three years imprisonment, or five years

prohibit the preventing or hindering access to a programme or data held on a computer, or impairing the operation of any programme or data held on a computer. The law also increased the maximum penalty for such cybercrimes from five to ten years and refined the definition of computer abuse to cover denial of service attacks.

Germany's August 2007 anti-hacking law, making hacking[35], denial-of-service, and computer sabotage attacks on individuals[36] illegal. The provisions extend criminal liability to the intentional "preparation of criminal offences" by producing, distributing, procuring etc. of devices or data designed for such purposes. Offenders could face sentences of up to ten years in prison for major offenses.

The United States Congress is considering legislation that would create a law that would establish that the use of spyware to collect personal information or to commit a federal criminal offense is a federal crime. If passed by and signed into law, it would authorise the appropriation of USD 40 million for the prosecution of violations of the new law from 2008 to 2011.[37] In addition, the US Federal Trade Commission (FTC) has actively pursued spyware companies using its authority under Section 5 of the FTC Act. The FTC has brought 11 law enforcement actions during the past two years against spyware distributors. These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.

private structures

ic initiatives

ia- Internet Security Initiative[38]

Australian Internet security initiative, administered by the

nitral trial of the Australian Internet Security Initiative commenced
mber 2005, with participation of six Internets service providers
The trial highlighted that the vast majority of customers are unaware
ir computers are infected by malware and are grateful for the
ce in making their computer secure. Since the trial commenced the
Industry Spam Code of Practice f a Code for Internet and Email
Providers has come into effect (16 July 2006). The code
ments the Australian internet security initiative, as it contains
ns that enable ISPs to disconnect a customer's computer if the
is not resolved by the customer.

States

example of public-private-partnership in the US is in critical
ucture protection, under the National Infrastructure Protection Plan
managed by the US Department of Homeland Security. The
ork under the NIPP includes a government entity ("Government
ating Council", GCC) made up of government agencies and industry
("Sector Coordinating Council", SCC) in each of the determined
infrastructure sectors, including the Information Technology and
nications sectors. The NIPP is a framework for assessing and
ng the risk to each of the sectors, including threat, vulnerabilities,
sequences.[40]

other example of public-private domestic co-operation is the US
GARD programme to improve and extend information sharing
private industry and the government, including law enforcement,
ts to critical national infrastructure.

ally, the US National Cyber-Forensics and Training Alliance, is a
rtnership between law enforcement, academia, and industry that
ates on cybercrime issues. The Alliance facilitates advanced
, promotes security awareness to reduce cyber-vulnerability, and
s forensic and predictive analysis and lab simulations.[41]

tional initiatives

l of Europe/Microsoft

ıishing Working Group

Anti-Phishing Working Group (APWG) is a volunteer–run
um of industry and law enforcement focused on eliminating the
from phishing, pharming[42] and e-mail spoofing of all types The
has over 2 600 members including 1 600 companies and agencies as
national and provincial law enforcement It provides a forum to
phishing issues, define the scope of the phishing problem in terms
, and share information and best practices for eliminating the
.[43] The APWG website provides a public resource for reporting
attacks. When phishing is reported, the APWG analyses the
tion provided and adds it to its online phishing archive The APWG
orks to share information about phishing attacks with law
ment when appropriate In addition to phishing, the APWG tracks
-based Trojans, keyloggers and other malware

ing Anti-Abuse Working Group[44]

Messaging Anti-Abuse Working Group is a global organisation
on preserving electronic messaging from online exploits and abuse
goal of enhancing user trust and confidence, while ensuring the
bility of legitimate messages With a broad base of Internet Service
rs (ISPs) and network operators representing over 600 million
es, key technology providers and senders, MAAWG works to
messaging abuse by focusing on technology, industry collaboration
lic policy initiatives

oft's Botnet Task Force

ough its international Botnet Task Force, first held in 2004,
oft provides training to law enforcement officials from around the
who have been confronted with the task of investigating Botnet
Charney, S , 2005)

ank

hTank is a free community site where anyone can submit, verify,
d share phishing data PhishTank is an information clearinghouse,
rovides accurate, actionable information to anyone trying to identify

pyware Coalition (ASC)

ASC is a group composed of anti-spyware software companies, cs, and consumer groups which focuses on the development of l definitions in relation to spyware. On 25 January 2007, ASC ed working documents on best practices[45] aimed to detail the process h anti-spyware companies identify software applications as spyware potentially unwanted technologies.

sector partnerships

example of private sector partnerships in the United States is the and continued development of the Information Technology tion Sharing and Analysis Center (IT-ISAC). The IT-ISAC is a community of security specialists from companies across the tion Technology industry dedicated to protecting the Information ogy infrastructure that propels today's global economy by ing threats and vulnerabilities to the infrastructure, and sharing best s on how to quickly and properly address them.[46]

rds and guidelines

e of Electrical and Electronics Engineers (IEEE)[47]

IEEE is a non-profit organisation for the advancement of ogy. Through its global membership, the IEEE is a leading authority eas ranging from aerospace systems, computers and munications to biomedical engineering, electric power and consumer ics among others. Members rely on the IEEE as a source of l and professional information, resources and services. The IEEE is g developer of standards for telecommunications and information ogy.

tional Standards Organisation (ISO)

International Organization for Standardization (ISO) is a worldwide on of one national standards bodies from more than 145 countries, a non-governmental organisation established in 1947 and based in

ıe activity. ISO's work results in international agreements which are d as International Standards and other types of ISO documents.

ıe relevant ISO/IEC standards include the following.

ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management

ISO/IEC 19770-1 Software Asset Management: Are You Ready?

une 2007, the ISO and IEC joint technical committee (JTC) 1 mittee (SC) 27 proposed a new work Item on "Guidelines for curity (27032)".[48] This standard would provide comprehensive es on cybersecurity[49] to both service providers and users ations and end users) and, in particular address behavioural, ational and procedural issues. More specifically, it would offer 'best ' guidance in achieving and maintaining security in the cyber ment for audiences in a number of areas, and address the nent for a high level of co-operation, information-sharing and joint n tackling the technical issues involved in cybersecurity. This needs hieved both between individuals and organisations at a national level rnationally.

al Institute of Standards and Technology

nded in 1901, NIST is a non-regulatory federal agency within the artment of Commerce. NIST's mission is to promote US innovation dustrial competitiveness by advancing measurement science, ds, and technology in ways that enhance economic security and quality of life. In November 2005, NIST published the *Guide to e Incident Prevention and Handling* as NIST Special Publication 0-83.[50]

Wide Web Consortium

World Wide Web Consortium (W3C)[51] is an international um where member organisations, a full-time staff, and the public gether to develop web standards. W3C's mission is "To lead the Wide Web to its full potential by developing protocols and guidelines ure long-term growth for the Web."

cal solutions and resources

domestic initiatives

Cyber Clean Center (CCC)

006, the Japanese government began a project to reduce the number
nfected computers in Japan with the objective of preventing spam e-
d cyber attacks in Japan. To accomplish this, Japan has created a bot
tool known as "CCC cleaner" which can be downloaded free of
t *www.ccc.go.jp*

rent results from the project include 31 000 trapped bot programmes
nique) and 1 300 bot programmes reflected in the removal tool. To
total of 57 000 users in Japan have downloaded the removal tool.
ps for enhancing the project could include changing the composition
ypots and broadening the reach of ISPs.

– Automated Security Update Programme (ASUP)

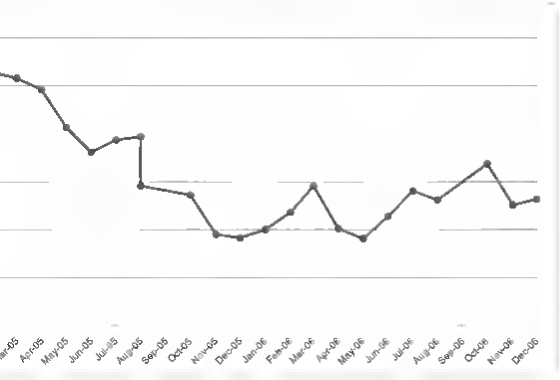
reduce the damage from vulnerabilities in Microsoft Windows,
Internet Security Center (KrCERT/CC) and Microsoft Korea
ated to develop and deploy the Automated Security Update
mme (ASUP) to home and SME users. The programme seeks to make
net connected information systems install Windows security related
without user intervention once they have installed ASUP. When
sit major Korean websites, such as portals, online game sites, a
window appears in the screen to confirm the installation of the
While offering the same functionality as Windows automatic
ASUP allows users to just click once to approve ASUP installation
having to modify the configuration of Windows updates.[52]
oft Korea has distributed the programme in accordance with
oft headquarters centralised patch policy, balancing user convenience
pany's philosophy on security.

le System

sinkhole system works to prevent bots from connecting to botnet
d and control (C&C) servers by subverting the IP address of the

As shown in Figure 8.1, after the adoption of this sinkhole system in
e botnet infection rate of Korea has reportedly dropped to almost
d at the end of 2005, compared with that of January or February

Figure 8.1 Botnet infection rate of Korea (2005-2006)



der

additional countermeasure used by KrCERT/CC is the
entation of MC Finder which locates malware on compromised
. MC Finder identifies an average of 500 exploited websites every
n Korea. KrCERT/CC is sharing the malware patterns with Google
e Korean major portal companies

ny effective technical solutions and resources have been developed
at threats relating directly or indirectly to malware. Some examples
solutions and resources include the following.

n Name System Security (DNSSEC)

SSEC applies cryptography to the Domain Name System to

signatures to authenticate DNS information. Many countries are to deploy DNSSEC at the ccTLD. For example, Sweden, Bulgaria, erto Rico have moved their country code TLDs to DNSSEC; r, it is important to have government, business, banking, and registry ation to successfully implement DNSSEC. There are currently experimental tests of secure DNS zones. It is recognised that C will not eliminate all misuse of the DNS. Some consider that it eal private information from DNS databases and therefore pose legal es for deployment in some countries.

n level authentication

main-level authentication is a means to enable a receiving mail server y that an e-mail message actually came from the sender's purported In other words, if a message claimed to be from *abc@ftc.gov*, the market authentication proposals would authenticate that the message rom the domain "ftc.gov", but would not authenticate that the came from the particular e-mail address "abc" at this domain. tically, if a phisher sent e-mail claiming to be from citibank.com, sage would be filtered by ISPs because the message would not have om a designated Citibank mail server. Consequently, ISPs and other s of receiving mail servers could choose to reject unauthenticated e- subject such messages to more rigorous filtering.

ltering[53]

ering is the most common technical anti-spam technology. The main of filters are the ease of implementation and the flexibility that users deciding which messages should be treated as spam. Heuristic filters that users specify criteria, such as keywords or a sender's address l prompt the filter to block certain messages from reaching the er's inbox. Spammers who deliberately misspell words or spell them erent language easily outsmart the keyword approach. More recent earn based on experience. They create statistics about each user's s in a recognition table for future reference to distinguish between d legitimate mails. The filter then lets through only messages that e the user's previous legitimate mail.

on Vulnerability Exposure (CVE)[54]

E is a dictionary of standardised names for vulnerabilities and other tion security exposures freely available to the public. The goal of to standardise the names for all publicly known vulnerabilities and exposures. CVE is a community-wide effort sponsored by the US ment.

on Malware Enumeration (CME)[55]

E provides single, common identifiers to malware threats in the wild e public confusion during malware incidents. CME is not an attempt ce the vendor names currently used for viruses and other forms of , but instead aims to facilitate the adoption of a shared, neutral g capability for malware.

t Engineering Task Force (IETF)

Internet Engineering Task Force (IETF) is a large open international nity of network designers, operators, vendors, and researchers ed with the evolution of the Internet architecture and the smooth n of the Internet. The actual technical work of the IETF is done in ing groups, which are organised by topic into several areas (*e.g.* transport, security, etc.). Much of the work is handled via mailing e IETF holds meetings three times per year.

Wide Web Consortium

World Wide Web Consortium (W3C)[56] is an international um where Member organisations, a full-time staff, and the public gether to develop web standards. W3C's mission is "To lead the Vide Web to its full potential by developing protocols and guidelines ure long-term growth for the Web."

Notes

e Annex A Background Data on Malware

ne example of such a scheme is the Common Malware Enumeration ME), the last notification of which was published on January 19, 2007 ee *http://cme.mitre.org/data/list.html* – it is difficult to know whether e delay in assigning CME references is a result of political problems ith the project, a lack of co-operation from vendors, or attacks becoming ore targeted and therefore falling outside the original scope of malware at CME addresses). Some experts consider that tracking malware nsistently across the industry is as large a problem as it was several ars ago or even greater today due to the significant increases in the mber of in-the-wild samples. Therefore, the problem of common alware identifiers is an issue that could still need to be addressed actically.

e "Instruments, Structures and Initiatives that Address Malware" low

ne revised ESNA can be found at
ww.dbcde.gov.au/__data/assets/pdf_file/0011/71201/ESNA_Public_Poli _Statement.pdf

formation available at
ww.dcita.gov.au/communications_and_technology/publications_and_re orts

formation available at *www.nctalert.gov.au*

formation available at
tp://ec.europa.eu/information_society/activities/sip/index_en.htm

formation available at *www.getsafeonline.org/*

etSafe at *www.netsafe.org.nz* is an initiative of the Internet Safety Group SG)

formation available at *www teenangels org/index html*

ouncil of Europe (2001), Articles 2, 3, 8

2006, Microsoft offered a substantial contribution to the Council of urope to finance the Convention's implementation programme

he European Network and Information Security Agency (ENISA) ovides a comprehensive directory of CSIRTS/CERTs in Europe at *ww enisa europa eu/cert_inventory/index_inventory htm*

2006, CERT/CC began hosting an annual meeting of CSIRTs with ational responsibility, see *ww cert org/csirts/national/conference2007 html* They also keep a list CSIRTs with national responsibility at *ww cert org/csirts/national/contact html*

nnish Communications and Regulatory Authority (FICORA) 9 B/2004 , available online at *ww ficora fi/attachments/englanti/1156489108198/Files/CurrentFile/FI ORA09B2004M pdf*

ederal Information Security and Management Act (FISMA), *ww pearlsw com/resources/Experts/OMBRequirements pdf*

vailable online at *www first org*

PCERT website *www apcert org/about/structure/members htm*

GC members include Finland – CERT-FI, France – CERTA, Germany CERT-Bund, Hungary – CERT/Hu, Netherlands – GOVCERT NL, orway – NorCERT, Sweden – SITIC, Switzerland – SWITCH-CERT, nited Kingdom - UNIRAS/NISCC

formation available at *www terena org/activities/tf-csirt/*

formation available at *http://stopspamalliance org/?page_id=11*

terpol includes 186 member countries, *ww interpol int/public/icpo/default asp*

formation available *www interpol int/Public/TechnologyCrime/WorkingParties/Default asp europa*

he *Information Technology Crime Investigation Manual* This manual is gitally available via Interpol's restricted website

formation available at *www londonactionplan com*

ıropean Union (2005)

troduced ınto UK law ın November 2006

ıe law deftnes hacking as penetratıng a computer securıty system and ınıng access to secure data, wıthout necessarıly stealıng data

xısting law already lımıts sabotage to busınesses and publıc authorıtıes

ongressional Budget Office Cost Summary (2007) p 1

formation available at *ww acma gov au/WEB/STANDARD//pc=PC_100882*

ıe followıng ISPs have now also joıned the ınıtıatıve Access Net ustralıa, AUSTARnet, Bekkers, Charıot, ınet, OzEmaıl, Powerup, ıhug, Net, Internode, Agıle, Neıghbourhood Cable, ıPrımus, Prımusonlıne, otkey, AOL, Reynolds Technology, Riverland Internet and Soul

ıe NIPP is available at *ww dhs gov/xprevprot/programs/edıtorıal_0827 shtm*

formation available at www ncfta net/default2 asp

ıarmıng" (or "warkıtıng") uses sımılar technıques as a classıc phıshıng tack, but ın addıtıon redırects users from an authentıc website (from a nk for ınstance) to a fraudulent sıte that replıcates the orıgınal ın pearance When a user connects ıts computer to, for ınstance, a bank eb server, a hostname lookup ıs performed to translate the bank's omaın name (such as "bank com") ınto an IP address contaınıng a serıes numbers (such as 193 51 65 37) It ıs durıng that process that maılcıous tors wıll ınterfere and change the IP address See OECD (2008b)

formation available at *www antıphıshıng org/ındex html*

formation available at *www maawg org*

formation available at *ww antıspywarecoalıtıon org/documents/BestPractıces htm*

formation available at *http //www ıt-ısac org*

formation available at *www ıecc org*

ıs work ıtem ıs stıll ın a development phase as of Aprıl 2008 For more formation, see *tp //tsotc tso org/ltvelnk/ltvelnk/fetch/2000/2122/327993/755080/1054 4/2541793/JTC001-N-8620 pdf?nodeıd=6542097&vernum=0*

defined by the proposed standard, cybersecurity refers to "the

formation available at *http://csrc.nist.gov/publications/nistpubs/800-/SP800-83.pdf*.

formation available at *www.w3c.org*.

uring the installation of Windows XP, users are asked to specify the tting of Windows Updates (Use Automatic Windows Updates or Notify ater). To protect users who inadvertently choose the "notify later" option rCERT/CC developed the AUSP programme with Microsoft Korea. Just installing the ActiveX control, users get protection from system ulnerabilities.

e OECD (2006).

formation available at *http://cve.mitre.org/*.

formation available at *http://cme.mitre.org*.

formation available at *www.w3c.org*.

Chapter 9. Possible Next Steps

s book has only begun to lay the foundation for understanding the e phenomenon and how it is evolving. Further work in many areas nd should be done to reach a better understanding. Fighting malware lex and would benefit from more comprehensive measurement, co- on and policy solutions. While many ongoing initiatives[1] are ting important resources to combating malware, there remain a of areas for improvement.

rtnership against malware

e need for a consistent approach to a global problem is not new, but e presents particular complexities due to the wide variety of actors sponsibility for combating malware. The communities involved in malware, whether governments, businesses, users, or the technical nity, need to improve their understanding of the challenges each of aces and co-operate – within their communities and across nities – to address the problem. Furthermore, their co-operation must the global level. It is not enough for one country or one community ively self organise if others do not do so as well.

ight of the need for a holistic and comprehensive approach to e, a common point of departure from which to build co-operation and e action could be to launch at the international level a global "Anti e Partnership" involving government, the private sector, the l community, and civil society. Such collaboration across the communities involved with fighting malware could benefit from the ice gained from developing the OECD's Anti-Spam Toolkit.

erent international public and private organisations including the and APEC could partner and lead the work in their area of

nprovement and further exploration

cifically, the "Anti-Malware Partnership" could examine the ng elements

ve prevention strategies

s element could examine all or part of the following

Reduction of software vulnerabilities (*e g* secure software development could be encouraged, governments could maximise their influence as buyers of software by requiring more secure software products as part of their procurement process).

nerabilities can be discovered by researchers either in the private r academia or by malicious actors with a motive for profit, or to a targeted attack for espionage or other purposes. Most vendors[2] the use of 'responsible vulnerability disclosure' practices in which ers inform the vendor about newly discovered software oilities and delay public disclosure to an agreed time to allow the ime to develop an appropriate software fix (patch).

ole behaviour by researchers could be promoted, for example by g the affected company first rather than going public before a solution le

hing is one way to mitigate against malware, but it is a reactive . Building security into the process for developing software would e a more effective and comprehensive long-term solution. Software be developed correctly the first time to minimise the occurrence of defects. The time frame between the discovery of a vulnerability ime of its exploitation is shrinking.

l efforts could be made to develop software that resists compromise ayered protections and separation of privileges. The use of security alidation methodologies for software products could also be promoted, propriate

nts could encourage the building of security in the development and n of software. They could also take advantage of their procurement of to foster the development of more secure software products

Awareness raising and education (*e.g.* further efforts should be made to improve online users awareness of the risks related to malware, and of the measures they should take to enhance the security of their information systems)

ny websites and resources exist to help end users and SMEs secure ormation systems but few of those programmes specifically address lain the problems of malware [3] Also, the number of resources can be elming to users as information and guidance can vary from entity to urthermore, some advice is inconsistent and may be inadequate in with the rapidly changing nature of the threat For example, advice olies that the only necessary countermeasure is keeping one's anti-tches up to date is inadequate

s efforts could continue to strive to provide information in plain so it can be understood by all participants, particularly those who have o technical knowledge or understanding. Given the continually nature of malware, any awareness activities would need to be updated or revised so that they remain effective. This would help to ome users and SMEs' online behaviour and practices with a view to heir ability to protect themselves from malware

The possibility to include security and abuse management in registrar accreditation procedures and contracts

Standards and guidelines (*e.g.* update of security manuals such as the IETF Security Handbook should be encouraged to include new challenges such as those presented by malware)

ndards, guidelines and good practice are important tools for the community. Those that are specific to malware or targeted at nities with responsibility to fight malware are particularly important re a comprehensive solution to the problem. For example, the Engineering Task Force's Security Handbooks which provide e for ISPs and users could be revised and updated to account for the

Research & Development (*e.g.* malware detection and analysis, security usability – how people interact with machines, software and online resources).

le this report does not attempt to examine the activities of the community, it is important to recognise their importance in ng malware. Both government and the private sector have a role in and conducting research and development (R&D) on a range of tion technology topics, including security risks.

d private sector R&D programmes focused on the security of on systems and networks could also consider malware

ring the malware problem

s element could examine and foster efforts to more accurately and ely measure the existence and impacts of malware.

ıy entities track, measure and sometimes even publish data on their ıce with malware and related threats.[4] However, vendors, CSIRTs, business community all have different data and ways of measuring gnitude of the malware problem and its associated trends. nore, there are many types of malware and little consistency of conventions in the technical community for identical types of . While existing data is helpful in understanding parts of the problem, it is not easily comparable in real and absolute terms.

orts should be made to more accurately and consistently catalogue, and measure the existence of, affects from and impact of malware.

olicies and practices

ois data is an important resource for attributing incidents of malware, refore it should remain accurate and accessible to law enforcement.[5] nore, malicious actors often abuse domain name registration such as ICANN's "add-grace period" or the minimal information nents set out by some domain name registrars (DNRs), to avoid n by authorities.

re are numerous DNRs that all have different policies and practices
essing malicious online activity. For example, there are 250 country
p Level Domains (ccTLD) in the world that set their own policies,
re not necessarily harmonised or co-ordinated. These different
s and policies may result in a different outcome each time a DNR is
take action against malware.

*uld be encouraged to develop common codes of practice at the national
national levels in co-operation with other stakeholders.*

s the case with DNRs, there are thousands of ISPs that all have
t policies and practices for addressing malicious online activity. ISPs
aps the best placed actors in the chain to help stop some types of
attacks, such as DDoS and botnets sending spam.

le many ISPs are working to improve security policies, some tend to
higher than average amount of malicious activity. These different
s and policies may result in a different outcome each time an ISP is
o take action against malware, which impairs the ability to fight
malware in an effective and consistent manner.

*d be encouraged to develop common codes of practice at the national
national levels in co-operation with other stakeholders*

ration for improved response

s element could examine the following:

Co-operation among CSIRTs (computer security incident response teams) (*e.g.* CSIRTs with national responsibility could share points of contact and work collectively to improve information sharing).

Codes of practice (*e.g.* a common code of practice for ISPs could be developed at the national and global levels in co-operation with governments; likewise, a common code of practice for DNRs (domain name registrars) could be developed at the national and global levels in co-operation with ICANN, the Internet community as well as others, as necessary).

ıth national responsibility could be encouraged to improve cross-formation sharing mechanisms for effective protection, detection and against malware

sonal contacts within informal trust networks enable the security e community to, for example, get an ISP to quickly act on a case of There is not one informal network, but rather several, which may be ping An ISP may approach a contact at a national CSIRT in another in order to get in touch with the relevant representative at an ISP in ntry. These contacts are reciprocal They are also contacted about n their own network and are expected to act on that information play a critical role as the first line of defence against attacks using Possibly one important role of a national CSIRT would be to also ormal Point of Contact (POC) for handling IT incidents affecting the ient and to receive requests for mutual assistance across ions

establish CSIRTs around the world could continue, especially where ot exist at the government or national levels, and consideration could o designating them as the Point of Contact for national co-ordination national co-operation against malware

ed legal frameworks

nd regulations

rnational harmonisation/interoperation of cybercrime laws is L Widespread adoption of the Council of Europe's Convention on me may be effective in this respect While 25 out of 30 OECD countries have signed the Convention, only 9 of those 25 have ratified it Furthermore, out of 21 APEC economies only 3, which Members of the OECD, have signed the Convention and of those 3 as ratified the Convention The Convention provides a framework peration and is a general commitment to co-operate internationally cybercrime

n to ratifying the Council of Europe's Convention on Cybercrime,

hened law enforcement

s element could examine the following.

Government efforts to provide mutual assistance and share information for the successful attribution and prosecution of cybercriminals.

Co-operation between CSIRT teams and law enforcement entities.

ources necessary for specialised cybercrime law enforcement s to be able to investigate and prosecute cybercrime in co-operation ner concerned public and private stakeholders. Malicious actors take ge of the fact that many countries do not have adequate legal orks/cybercrime laws and cyber investigation capabilities. They also vantage of the complex challenges faced by law enforcement and response when working outside their jurisdictions which are ned by geographical boundaries. Cross-border information sharing law enforcement entities is a critical element of investigating and ting cyber criminals. While mechanisms such as the G8 24/7 ime Network provide for points of contact among such law ment entities, it is unclear how such networks co-operate among ves.

ause of the highly technical nature of malware, governments should egular training for judges, prosecutors and other law enforcement

ware analysis can play an important role in recovering evidence and ng leads for law enforcement to investigate cybercrime. Malware is often conducted using methods such as hard drive imaging, "real- forensics, antivirus testing, and reverse engineering (CERT ation Center, 2007). In some cases these practices may not be d under laws that protect intellectual property.

f laws that prohibit reverse engineering malware could be considered nforcement and research purposes, with appropriate safeguards for the n of owners of intellectual property.

re may be tensions between the protection of privacy and actions to lware. For example, CSIRTs may need to share information, such as

example, dismantle botnets and conduct investigation into the is activity.

ection laws could be applied in a way that does not prohibit the with the appropriate safeguards, of IP addresses and other information t be necessary for fighting malware

cal measures

s element could examine the following:

Technical measures such as filtering, DNSSEC, sinkholing and many others could be examined to understand how they would help fight malware.

How users might be provided with better tools to monitor and detect the activities of malicious code, both at the time when a compromise is being attempted and afterwards

ware presents complex technical challenges and therefore solutions bating it need to be supported by technical measures, such as , which may be an effective way to minimise the amount of nate traffic on the network. Some examples of existing technical s and resources are provided in Chapter 8.

fforts to develop and implement effective technical solutions to detect, nd respond to malware could be encouraged

ld be provided with better tools to monitor and detect the activities of code, both at the time where a compromise is being attempted and s.

nomics of malware

s element could examine the following:

How to strengthen existing security-enhancing incentives of market players.

Introduction of security-enhancing incentives through alternative

economic perspective on malware would provide policy makers and players with more powerful analysis and possibly a starting point for governmental policies related to incentive structures and market ities

following could, for example, be topics for further exploration

Effectiveness and economic effects of assigning alternative forms and levels of legal rights and obligations (*e g* liability) to the different stakeholders This would include legal constraints for ISPs to monitor and manage their networks (*e g* related to privacy, 'mere conduit', 'safe harbour' provisions)

Effectiveness and economic effects of blacklisting on ISP and end user security

Effectiveness and economic effects of global measures to strengthen law enforcement and collaboration in the area of malware

Effectiveness and economic effects of technological solutions to the problem of malware (*e g* 'security moving into the cloud' and 'tethered devices' for end users)

Strength of reputation effects and other feedbacks in mitigating the problem of information security

Efforts to quantify the magnitude of the overall social externality due to lack of trust in the e–commerce system (growth effects, GDP impact)

Better assessment of the strength of the trade-offs between usability, availability, functionality, performance, cost and security

Malware in next generation networks and system architectures (*e g* more mobile, EoIP-everything over IP-networks, Web 2 0)

Obstacles to and means to enhance incentives for information security of individual users

co-ordination and cross-border co-operation

s element could examine the following:

The cross-cutting need for information sharing, co ordination and cross-border co-operation.

Suggestions for disseminating the anti-malware guidance at the global level and following up on its implementation.

of the previously mentioned areas for action illustrate the cross- need for information sharing, co-ordination and cross-border co- n. However, the communities of actors described above do not collaborate in an effective manner to combat malware. Information and co-ordination among the private sector, the government and akeholders is not always adequate to detect, respond, mitigate and ropriate enforcement measures against malware. This can be at least attributed to the fact that no comprehensive international hip for collaboration against malware does yet exist despite the nt work underway. (See Chapter 8 for examples of existing onal co-operation).

more holistic approach involving an integrated mix of policy, nal procedure and technical defences could be considered to ensure ormation sharing, co ordination and cross border co operation are ely integrated and addressed.

y a holistic approach involving an integrated mix of policy, nal procedure and technical defences can ensure that information co-ordination and cross-border co-operation are effectively ed and addressed.

success of such a global "Anti-Malware Partnership" would require ngagement from all participants. Such an effort, however, would trate significant advances in the international community's ability to ne obstacles to addressing a global threat like malware through o-ordinated action.

ses to governments to end users While malware often propagates the Internet, it is important to remember that it is software which introduced into Internet connected and non-Internet connected r systems Malware whether used directly, or indirectly, to conduct is activity online erodes trust and confidence in the Internet and the conomy

2002 *OECD Guidelines for the Security of Information Systems and* s provide a list of broad information security principles all of which vant and applicable to the fight against malware The nine principles ness, Responsibility, Response, Ethics, Democracy, Risk assessment, design and implementation, Security management, Reassessment) participants at all levels, including at the policy and operational *The Guidelines* can and should be applied to the challenges raised by today

rapidly evolving nature of malware makes international co- n essential to addressing the problem This co-operation should be ed and enhanced by accurate and quantitative measurement of the and the underlying economics at play While this paper details the problems presented by malware, it is only a first step in moving a solution A holistic and multi-stakeholder proactive approach is to take advantage of all opportunities for improvement across the communities addressing malware

Notes

formation available at *www.w3c.org*.

s an example, Microsoft is one. See
ww.microsoft.com/technet/community/columns/secmgmt/default.mspx

dustry organisations, such as APACS, have reported no reduction in the vel of phishing due to awareness campaigns and public figures ghlighting the problems and scale of the attack. APACS (2006) ulnerability and threat assessment of authentication mechanisms used r Internet based financial services – 2006 review, page 3 and 4.

e Annex A, Background Data on Malware.

vil liberties groups have recommended that ICANN limit the use and ope of the Whois database to its original purpose and to establish its olicies based on internationally accepted data protection standards. ublic availability of Whois data may also conflict with the EU Data otection Directive, which limits access and collection rights to the tabase's original technical purposes.

Annex A. Background Data on Malware

hough malware as we know it today is a relatively new phenomenon
ed to the early days of worms and viruses, it is growing and evolving
essive rates. Trends in data show that while the categories of
used to conduct malicious activity (*i.e.* virus verses Trojan) change
lve over time, the use of malware is steadily increasing.

nputer Security Incident Response Teams (CSIRTs) or Computer
ncy Response Teams (CERTs), software and anti-virus vendors, and
nerally security companies are examples of entities that track and
the existence of malware. While the data provided below is helpful
erstanding elements of the malware problem, it is not easily
able in real and absolute terms and thus this paper does not attempt
comparisons or draw conclusions across disparate sets of data. This
is primarily intended to demonstrate the type of information
e and different analytical perspectives from the organisations listed

ed by CSIRTS

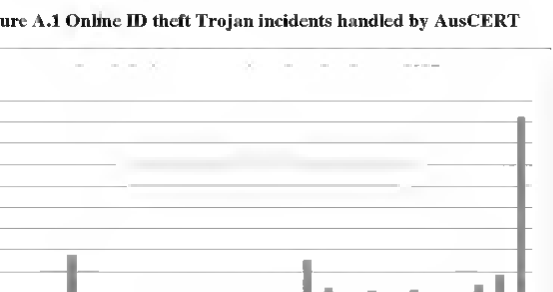
RT

CERT is the national Computer Emergency Response Team for
a. AusCERT provides computer incident prevention, response and
on strategies for members.

igure A.1, each incident represents a single unique URL or domain

en data. The number of IP addresses associated in a single incident ngle attack is variable but can range from 1 to around 100.

ure A.1 Online ID theft Trojan incidents handled by AusCERT



AusCERT (2006)

ure A.1 does not include specific compromised hosts involved in any ttack or incident – only URLs and domain names. Nor does this he number of computer infections (compromised hosts) that occur ach attack of which there are generally many hundreds or thousands.

high figures for July 2007 are due to the storm Trojan (often tly referred to as a worm). It does not automatically propagate and botnet C&C functionality, *inter alia*.

Brazil (CERT.BR)

RT.br is a national CERT which collects public statistics on the s that are reported to them voluntarily. For example, a home user ort when he/she received an e-mail that is clearly a fraud attempt, nk to a malware executable. CERT.br tests to see if the executable is line and then reports the occurrence to the host of the site. They also

Table A.1. CERT.BR Incident Reports

	Total number of incidents reported	Worm[1]	DoS	Intrusion[2]	Fraud[3]
	75 722	42 268	104	248	4 015
	68 000	17 332	96	448	27 292
	197 892	109 676	277	523	41 776

rm category are reports received of worm/bot propagation, *e.g.* port scans of ports used by worms/bots to propagate (445, 135, 5900, etc). These reports are t by firewall administrators and even home user using personal firewalls, etc. It nt to note that the worm category does not try to count machines infected by t incidents regarding worm propagation attempts.

n, according to CERT.BR classification, is a system compromise – this is t by the system owner/administrator and reported to CERT.BR. For example, a ver administrator sends CERT.BR a report saying his/her machine was sed, a rootkit was found, etc.

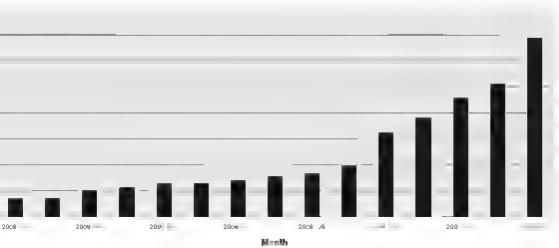
ud category refer to various fraud types: copyright infringements, credit card itional phishing and malware related fraud. The last one is the majority of the azil.

CC, United States

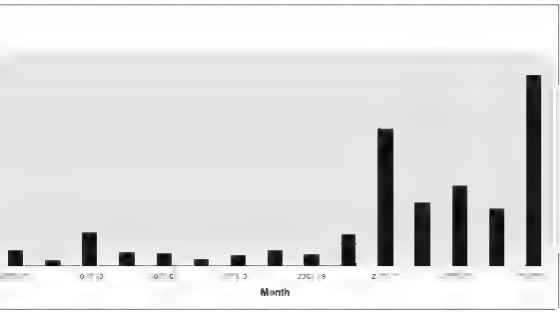
Computer Emergency Response Team Coordination Center CC) at Carnegie Mellon University collects data on malware from and private sources. Since 2006, CERT/CC has been collecting, g and cataloguing every piece of malware it is able to find that has stributed via the Internet or which otherwise has found itself onto r systems. While many malware artefacts have similar functionality, e is considered to be a unique variant if it generates a unique MD5 or ash function.[1] Therefore, some types of self-propagating malware viruses and worms which produce many thousands of identical would be counted as a single variant.[2]

ce the figures below from CERT/CC, while not necessarily e, are nonetheless significant in their depiction of malware trends, how an exponential increase in malware artefacts[3] from January March 2007. From less than 50 000 in January 2006, the total of artefacts rose to 350 000 in March 2007, as represented in Figure ow. For each month of the same period, Figure A.3 represents the

e A.2 Total artefacts by month from January 2006 to March 2007



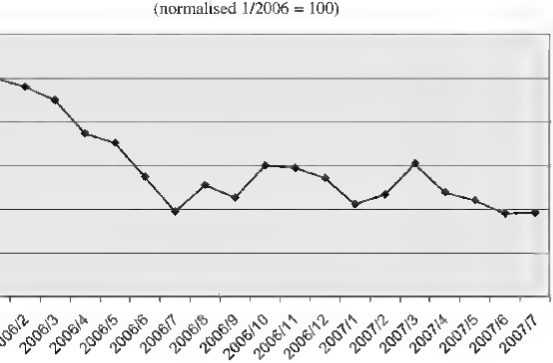
e A.3 New artefacts per month from January 2006 to March 2007



FI, Finland

RT-FI is the Finnish national Computer Emergency Response Team ask is to promote security in the information society by preventing, ng, and solving information security incidents and disseminating tion on threats to information security. Figure A.4 represents the andled by CERT-FI Abuse Autoreporter system, their automated ase processor. The graph is cases / month, normalised to 100 =

A.4 CERT-FI Abuse Autoreporter montbly case processing volume



T/CC

ERT/CC gathers data from honeynets[4] and incidents reports. n 2005 and 2006 data from both incident reports and honeypots a decrease in the number of worms and an increase in the number of eorses from 2005 – 2006 (see Figures A.5 and A.6)

re A.5 Incident reporting to KrCERT/CC by month (2005-2006)

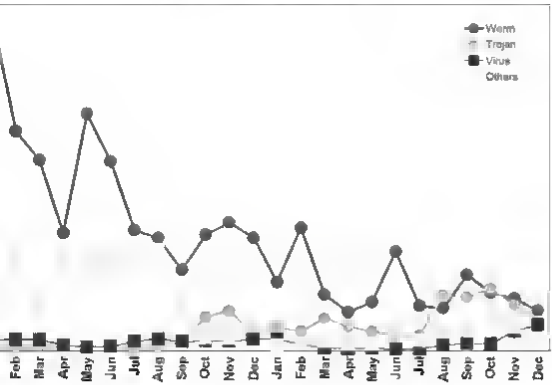
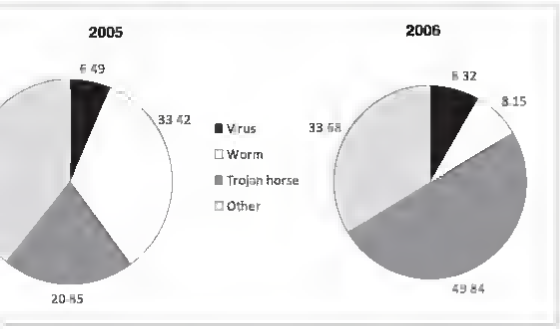


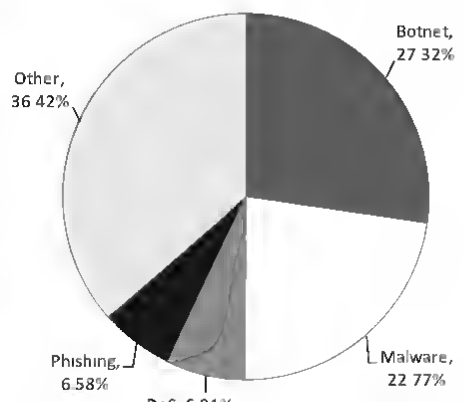
Figure A.6 Information gathered from KrCERTr boneynets



RT, Norway

ıan National Security Authority (Nasjonal sikkerhetsmyndighet –

Figure A.7 Incidents handles by NorCERT in 2007

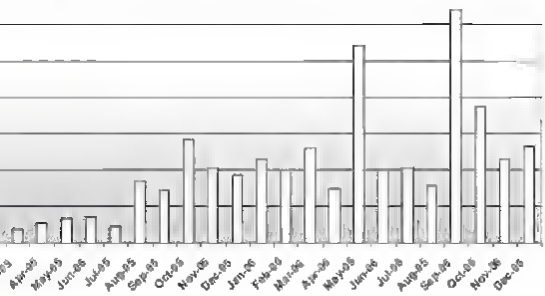


oftware and anti-virus vendors

ıtion of payment

ACS, the UK payments association, is a trade association for ons delivering payments services to end customers. It enables the o address co-operative aspects of payments and their development. It he main industry voice on issues such as plastic cards, card fraud, , e-banking security, electronic payments and cash. Working Groups co-operative areas such as developing authentication solutions and ng to attacks on e-banking customers. Figure A.8 tracks the number an incidents targeting UK banks from February 2005-December

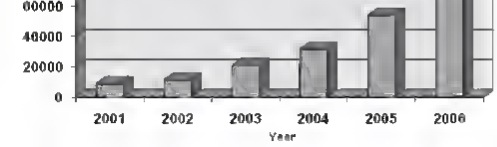
Figure A.8 Trojan Incidents targeting UK banks



sky Lab

persky Lab is an international information security software vendor. ky Lab is headquartered in Moscow. Kaspersky labs reported an ntial increase in previously unknown malicious programmes from 006, as illustrated in Figure A.9. They also reported a steady increase umber of Trojan spy programmes designed to steal information from nline accounts (Kaspersky Labs, 2006).

gure A.9 Increase in the number of new malicious programmes

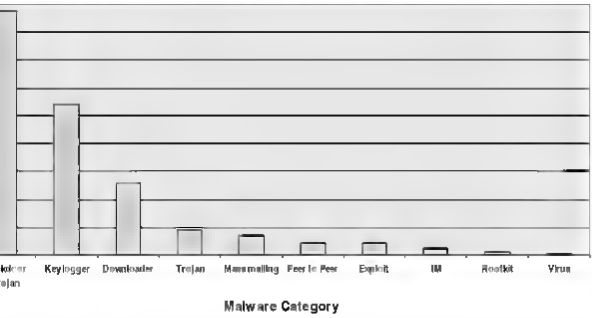


oft

rosoft gathers data from several anti-malware products and services
d on information systems running Microsoft products Based on
observed from January to June 2006, Microsoft reported the
e of more than 43 000 new malware variants between January and
2006 (Microsoft, 2006a) This can at least partially be attributed to
he availability of malware for purchase on the Internet, it is easier
kers to modify a piece of existing malicious code rather than create
family" of malicious code

rosoft also reported that among new malware variants backdoor
accounted for the highest number (see Figure A 10) The figures
trate that the four most common categories where new variants have
eated were of the non-self-propagating varieties, which are typically
ed with smaller scale cyber attacks aimed at illicit financial gain,
arly financial fraud

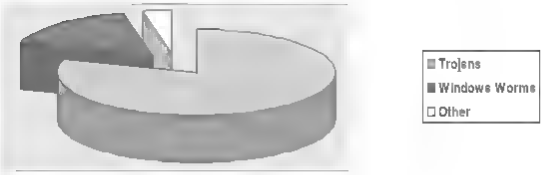
.10 Microsoft Malicious Software Activity from January - June 2006



OS

PHOS gathers data from 35 million users in 150 countries that

gure A.11 Trojans verses Windows Worms and Viruses in 2006



Source Supra Sophos (2007a)

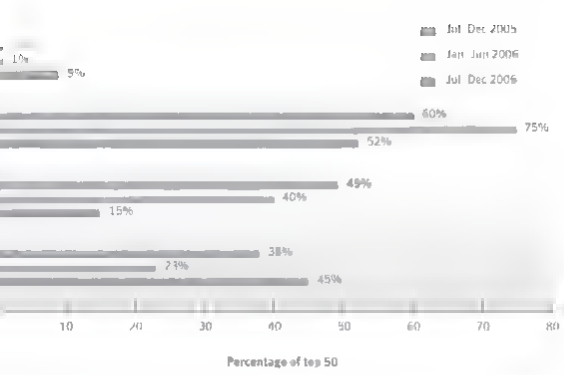
tec

antec gathers information from 40 000 registered sensors in 180 s, 120 million desktop computers, and gateway and server antivirus ions, and 2 million decoy accounts in the Symantec Probe Network ec operations are conducted from four security operations centres ht research centres. Symantec software products are deployed on an 370 million computers or e-mail accounts worldwide.

ently, Symantec reported a decrease in the amount of worms[5] and ors and an increase in the amount of viruses and Trojans.

ddition to this data, the Symantec Corporation reported an increase ously unseen malware, or new families. Between July and December ymantec honeypots discovered 136 previously unseen malware , an increase of 98 from the previous 6 months (Symantec, 2007). It rtant to note that while information gathered from honeypots and ts is useful, it is not necessarily representative of a global trend.

Figure A.12 Malicious code types by volume



Symantec (2007)

s on the data

data on malware presented above comes from a variety of very t and incomparable sources (national CSIRTs, software vendors, and vendors). The definitions, types of incidents, type of damage, time nd scope are not harmonised across these various organisations and e it is necessary to be prudent in comparing such disparate data.

wever, it is more or less possible to highlight certain tendencies that be shared: *i*) an significant and noticeable rise in security incidents to malware ; and, *ii*) Trojan malware becoming more and more t when looking across types of malware. As has often been , there are fewer serious outbreaks of worms and viruses and thus a rt of the increase in malware variants can generally be attributed to pagating varieties which usually have a more harmful /functionality and tend to be financially motivated.

agreement by certain stakeholders interested in measuring malware

n some of the data, it is possible to summarise and highlight several
o demonstrate that the problem of malware is becoming more and
gnificant

Box A.1 Summary of sample data on malware

e A.1 Total number of incidents reported ~ + 225%.

re A.2 Total artefacts in the last year ~ +250%

re A.6 Decline of Worms related incidents ~ -25%/, Increase of Trojan incidents ~ + 30%.

re A.11 Malicious programmes increase by 800% in the last 5 years

le it is true that many attack trends are increasing, it is unclear how ends relate to the overall damage caused of malware. Detecting a number of Trojan variants does not necessarily mean that there is amage. It could also be a response to improved security defenses y, signalling that large-scale botnets are shrinking in size does not ily mean that the counter measures are effective. It might be that s have found smaller and more focused botnets to be more le. In short because malicious attack trends are highly dynamic, it is to draw reliable conclusions from the trends themselves.

Notes

tackers often generate a new malware variant from an existing piece of alware by simply changing the manner in which the code is ompressed and packed', rather than changing the malware code itself or example, see: *tp //us trendmicro com/us/threats/enterprise/glossary/c/compression/in x php*. New variants produced in this manner are not each given a new ME number. Multiple variants, which are considered to be identical in nctionality and form will have the same CME number, whereas even nall variations in malware byte code will produce a new CME number, e http //cme mitre org/cme/process html

is approach is important as counting each infection from a single large orm or virus outbreak can skew the results and does not reflect the tual level of development of new variants by many attackers ecifically in order to evade detection by anti-virus products.

n artefact is a file or collection of files which may be used by versaries in the course of attacks involving networked computer stems, the Internet, and related technologies.

computer terminology, a honeypot is a trap set to detect, deflect or in me manner counteract attempts at unauthorised use of information stems. Generally it consists of a computer, data or a network site that pears to be part of a network but which is actually isolated, n)protected and monitored, and which seems to contain information or a source that would be of value to attackers. Two or more honeypots on a twork form a honeynet.

is drop can largely be attributed to the decline in reports of major orms such as Sober X, Blackmal E, and Netsky P75 since the first half 2006.

x B. Research Design for Economics of Malware

evaluation started with an exploration of the incentives at work in ıvidual organisation and those related to the decisions of other ng or complementary organisations The reliability of the tion is increased if interdependent stakeholders present compatible of the relevant incentives and their effects Attempts were made to w several organisations in each segment of the value chain to narratives that are as coherent as possible In a subsequent al step, these individual narratives were then integrated to assess the ncentive structure of the sector and the resulting externalities

llection

he course of 2007, we conducted 41 in-depth interviews with 57 onals from organisations participating in networked computer ments that are confronted with malware Firms from the following ents of the value net were approached:

Internet Service Providers

E-commerce companies, including online financial services

Software vendors

Hardware vendors

Registrars

Security service providers

Different types of end users

Governance institutions (regulators, consumer protection agencies, CERTs)

interviews were carried out using a semi-structured questionnaire, for the specific situation of the interviewee. In each instance, we how the organisation was confronted with malware, what its es were, what trade-offs were associated with these responses, and organisation was affected by the actions of other market players. As ion practice in the social sciences, we have treated all interview data dential, so as to enable the interviewees to share information with us y as possible. Consequently, no interviewee or organisation is d by name in relation to specific data and all quotes have been d by the respective individuals/organisations beforehand for ion. All statements in the report are based on interview transcripts er documents supporting the findings. Although this limits the direct lity from readily available public sources, we felt that given the ory stage of research in this area, our approach would enable us to r insights into market-sensitive economic data and decision making.

and limitations

ore turning to the empirical findings, it is important to note the scope tations of this study. The global and heterogeneous nature of the m of Internet services implies that any study of incentives is almost ssity an exploratory study. The limited time and budget available for ly allowed for a limited number of interviews in six countries. The of the interviews took place in the United States and the nds, with additional interviews in the United Kingdom, France, y and Australia. The next section presents our findings for five of ket players we interviewed:

We intended to also describe the incentives for hardware vendors

Internet Service Providers

E-commerce companies, including online financial services

Software vendors

Registrars

End users

t we were unable to secure sufficient interviews with hardware to provide the basis for such a description. The examination of the

le these interviews have proven to be highly informative, the drawn from them should be read with caution First of all, it is ble to assume that the set of interviewees is influenced by some of self-selection ISPs, for example, are more likely to respond bly to an interview request about the economics of malware if they urity policies in place that are at least on par with other ISPs, if not That said, some of the organisations we interviewed are publicly for a less than stellar track record with regard to security – which en explicitly acknowledged during the conversations Second, the al findings report on how stakeholders themselves describe what doing and why In other words, we report on the perceptions of the wees, not some independent assessment of their actions and the driving them Whenever possible, we did cross-check information d to us against the information from other interviews and against available data, such as security reports, surveys and research ions Third, the interviews touch on many issues that concern ary or otherwise confidential data. Interviewees were not always share this data with us and if they were, we were constrained in g them Fourth, and last, our interviews involved six different legal ions Some incentive mechanisms are generic but others are context- Our approach hence provided us with a sense of the degree to ertain findings were country-specific and therefore could not fully he heterogeneity of all OECD members

se circumstances make it more difficult to generalise our findings r, very little empirical field work has been done in this area so far of the rapidly increasing political attention given to the issue of and the policy initiatives currently under debate, this is a critical n Our study contributes to overcoming this omission At the very makes clear the urgency of developing a further-improved in-depth nding of the economics of malware to increase the probability of nterventions to succeed

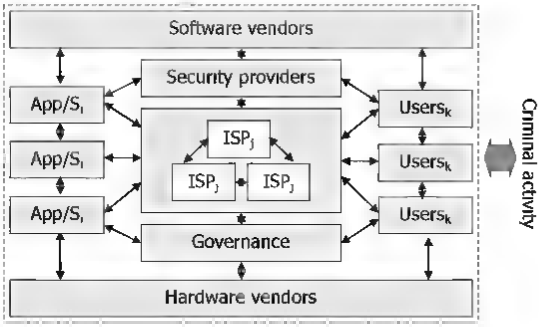
ex C. A Framework for Studying the Economics of Malware

information and communication technology (ICT) industries form a ecosystem, and their services permeate most other economic s Security problems and the related economic costs to society may vo roots: *i*) they are the outcome of relentless attacks on the tion and communication infrastructure by individuals and ations pursuing illegal and criminal goals; and *ii*) given an external vel, they may be aggravated by discrepancies between private and costs and benefits, which are the outcome of decentralised decision in a highly interrelated ecosystem. Both actors in the illegal and realms, as well as legitimate participants within the information and nications system, respond to the economic incentives they face.

his complex value net (see Figure C.1), economic decisions with o information security depend on the particular incentives perceived player. These incentives are rooted in economic, legal, and informal sms, including the specific economic conditions of the market, the endence with other players, laws and regulations, as well as tacit orms.

hin each participant's own purview and constraints each participant s rationally to a variety of incentives, even though the available tion may be incomplete. However, for the economic efficiency of le value system, it is critical that the incentives of the individual nts be aligned with the overall conditions required for societal cy. In other words, the relevant incentives should assure that the costs and benefits of security decisions match the societal costs and . In the case of differences between private and societal optimal es, the prevailing incentive mechanisms should ideally induce ents toward higher social efficiency.

Figure C. 1 Information industry value net



different types of application and service providers
different ISPs
different types of users (small, large, residential, business)

alignment between private and social efficiency conditions may take forms In case of incomplete information, the perceived incentives of al players may deviate from the optimal incentives A related issue roblem of externalities, systematic deviations between the private or costs and the societal benefits or costs of decisions Due to the gree of interdependence, such deviations from optimal security s may cascade through the whole system as positive or negative ities

the research on the economics of crime has illustrated, criminal s may be analysed in a market framework The activities in the for cybercrime and cybersecurity are closely interrelated Before the of incentives and externalities can be explored in more detail, we erefore, briefly explore the working of these markets and their

lysis of cybercrime

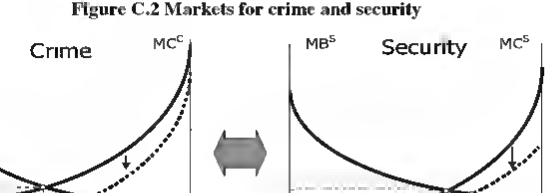
criminal activity Franklin *et al* (2007) also employ an economic ork to study an underground economy based on "hacking for profit" se a slightly different representation than these studies, based on l analysis It is reasonable to assume that a higher level of security is is only possible at increasing cost Furthermore, it is likely that tional cost will increase more than proportionally as the extent of violations increases.

he other hand, the marginal benefits of additional security violations creasing function of the level of violations This is an expression of that the most lucrative crimes will be committed first, and that al criminal activity will only yield lower marginal benefits ls will extend their activities until the marginal cost of additional violations approximates their marginal benefits The magnitude of fits and costs of crime is dependent on a number of variables, some n are affected by private and public measures to enhance security A xamination of these factors allows comparative assessments of outcomes. It also sharpens understanding of the principal nities to intervene in the market to reduce cybercrime

hnological change, the increased specialisation and sophistication in duction of malware, and the globalisation of the information and nication industries have all reduced the marginal cost of crime [1] In s cost decrease has dramatically expanded the supply of crime, as from countries and regions with low opportunity cost of labour increase the net benefits of crime) join criminal activities Such marginal costs of security violations will shift the marginal cost of chedule downwards Assuming that other things, especially the relationship, remain unchanged, reductions in the marginal cost of ill result in a higher level of security violations and vice versa

hnological change and globalisation have also increased the benefits e. For example, the wider reliance on e-commerce and credit card ions has increased the opportunities to exploit technical and personal loopholes. The globalisation of the Internet has also enabled s to reach a larger number of potential victims. These changes shift ginal benefit curve upwards (not captured in Figure C.2) Other eing equal, this increase in the marginal benefits results in a higher security violations The presence of both effects explains much of eased level of activity of security violations In principle, however,

Figure C.2 Markets for crime and security

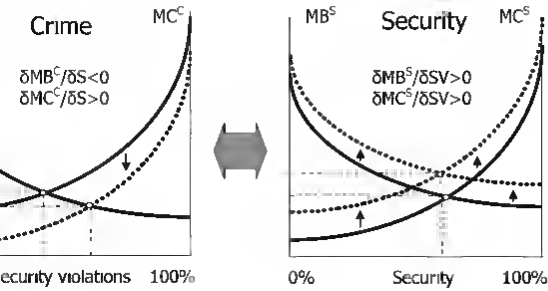


rket for cybersecurity

market for security can be analysed using a similar approach It is ble to assume that higher levels of security can only be achieved at narginal costs On the other hand, the marginal benefits of security rease Unless the benefits exceed the cost throughout, the resulting level of security will be below 100%, at least on an aggregate level.[2]

nges in the costs of providing security and the benefits of having will shift the marginal cost and benefit schedules and affect the outcome A reduction in the cost of security, for example, due to the lity of more efficient and cheaper filtering software or a new architecture that might reduce the propagation of malware, will hings being equal) result in a higher level of security Likewise, benefits of security, perhaps because of the utilisation of more critical applications, will (other things being equal) result in a level of security However, such initial changes may result in ent adjustments by other actors, who might reduce their expenditure rity in response, leaving the overall effects on the resulting security ambiguous at best (see the arguments in Kunreuther and Heal, 2003)

Figure C. 3 Markets for crime and security



marginal benefits of crime
marginal costs of crime
marginal benefits of security
marginal costs of security

S<0 expresses the changes of the MBC curve in response to a change in the security S The negative sign implies that the marginal benefits of crime move opposite direction from marginal changes in security, *i e* increased security he marginal benefits of crime, all other things being equal

ion of cybercrime/cybersecurity

markets for cybercrime and security are highly interrelated (Figure ctivities in the market for cybercrime affect the market for security e versa Most likely, an increased level of security violations will the marginal benefits and the marginal costs of security, shifting edules upwards On the contrary, a lower level of security violations from the market for crime will shift both schedules down On the nd, variations in security will have corresponding effects on the for crime Increased security will increase the marginal cost of violations, and it will reduce the marginal benefits of crime.[3] The act on the overall level of security is difficult to predict and will on the relative strengths of variations in security violations on the d benefits of security A higher level of security violations could a lower level of security, an unchanged level of security, or even a

l of security. But for all actors it will likely result in higher costs for ing a certain level of security. On the other hand, a higher level of will induce changes in the market for crime in that it will increase ginal cost of security violations and, at the same time, reduce the l benefits of crime. Both effects will mutually reinforce each other, tributing to a lower level of security violations. Since parameters in the markets change continuously, the outcomes of the resulting mutual adjustment are difficult, if not impossible, to model, n the directions of change seem to be robust.

narket analysis

narket analysis framework can give high-level insights into the s available to influence overall outcomes. Such measures can target ket for cybercrime and/or the market for security. Measures such as ng the cost of cybercrime by increasing the associated penalties, ening national and international law enforcement, and increasing the y of registering and maintaining fraudulent domains and websites, ct the market for crime directly and also have repercussions on the for security. Most likely, such measures will reduce the overall level rity-related costs. For reasons discussed above, it is less certain that easures will increase the level of security, since accepting a certain insecurity is economically rational.

asures affecting overall incentive compatibility in the security range from forms of industry self-regulation to forms of co- on and government intervention. They encompass a wide spectrum ures, such as: requiring that security features are enabled by default, endations to ISPs to adopt best practices with regard to security on tworks, information campaigns to alert users to security risks, and in the ways domain names are registered. None of these measures is ea, but they help better align individual incentives with societal cy requirements.

ncentives: what they are, how they work

nomic incentives are the factors that influence decisions by uals, as well as organisations. A close examination of the incentives

es in case an intrusion has happened or an attack is unfolding The set of incentives is most likely different for each stakeholder we attempted to get a detailed account of the incentives as perceived cipants in the information industry Moreover, the incentives may nent each other, they may form a trade-off, or they may even work -purposes An important goal of our analysis was, therefore, to the aggregate interaction of the individual incentives faced by ders at the sector level Since systems of incentives have many k loops, it is typically very difficult to determine the net effect of a of incentives At this initial stage of the field research project, we ualitative approach

nomic incentives shape decisions in for-profit commercial firms, fit social groups, public and private sector governance institutions, as not-for-profit forms of production and collaboration Incentives n classified in monetary (remunerative, financial) and non-monetary ancial, moral) terms Financial incentives include factors such as e salary of an employee to corporate performance, the ability to super-normal profit by pursuing a risky innovation, or the bottom ects of potential damage to a firm's reputation Non-financial es encompass norms and values, typically shared with peers, and a common understanding as to the right course of action or the set ble actions that should be avoided in a particular situation Financial es typically connect degrees of achievement of an objective to y payments Non-financial incentives work through self-esteem (or d community recognition (or condemnation)

ractical decision making, incentives can be seen as the motives for g a specific action or the rationales for preferring one course of ver another As the discussion of reputation effects illustrates, it is ies necessary to distinguish between short-term and long-term Characteristic features describing incentives are their power (low- l to high-powered) and directionality (positive or negative relation to f decision).[4] An important question is the relation between the e and power of the relevant incentives and the objectives of s.

full set of incentives at work typically consists of a bundle of , more narrowly defined, incentive mechanisms These incentive isms may work in the same direction or conflict with each other If

tion security but potential first-mover advantages in the information es may, *ceteris paribus*, lower the incentives to invest in information

ntive-compatibility refers to a situation in which an incentive is ed in a way as to contribute to the stated goals of an individual or an ation. To assess incentive compatibility, the direct and indirect links an incentive mechanism and the objective being pursued will have Examined. Incentive compatibility may exist at the level of a single e mechanism, the bundle of incentives at work for a specific der, or the entire sector under consideration. Given the potential for fs and even direct conflicts between incentives, incentive bility is much more difficult to ascertain at the level of stakeholders industry at large. It is a particular challenge in an industry as highly ated as advanced information and communication industries are. To ted by an incentive mechanism, individuals need to be cognizant of ence, its directionality, and its power. Incentives that exist on paper gnored by the decision makers must either be seen as zero-powered relevant incentives. Therefore, it is possible to reveal the existing e structures of the stakeholders in the information value net by xperts and decision makers for an in-depth account.

s

rnalities are forms of interdependence between agents that are not d in market transactions (payments, compensation). Which ena are identified as externalities depends to a certain degree on the ation of legal rights and obligations in the status quo. If these rights gations are only vaguely defined they may need clarification by ures, courts and in private contractual agreements.[5] If such tion is afflicted with transaction costs, rational individual actors by the externalities will not internalise them if these costs exceed ntial benefits of internalisation. In this case, only a collective actor business association, government) may be able to address these ensated externalities.

the formulation of the mainstream economic model, these endencies lead to deviations from a socially optimal allocation of s. Negative externalities result in an overuse or overproduction

r to consumer, consumer to producer and consumer to consumer
ities (Just *et al*, 2004)

alternative typology distinguishes between technological and
y externalities (Nowotny, 1987, p. 33). Technological externalities
to exist if, at constant product and factor prices, the activities of one
rectly affect the activities of another. Pecuniary externalities exist, if
vities of one agent affect the prices that need to be paid (or may be
) of other agents. Early contributions to the subject, for example, by
l (1920) or Pigou (1932), treated externalities as an exception, a rare
y in a market system. However, the increasing concern with
mental issues since the 1960s made clear that such interdependencies
asive and part and parcel of real world market systems.

s is particularly true for information and communication networks,
raise several new and unique issues. The high degree of
nectedness amplifies the interdependencies between participants in
work. Both negative and positive effects that are not reflected in
transactions may percolate widely and swiftly through electronic
nication networks. In some types of networks, such as peer-to-peer
ments, agents take on dual roles as consumers as well as producers
rmation and other services. Many users of cyberspace view it as a
us, in which transactions take place according to a gift rather than
lace logic. Moreover, often, for example, in the case of Trojans,
ities are generated without the explicit consent or knowledge of an
al user. All these factors influence the prevalence of externalities
plicate possible ways to address them.

xternalities in networked computer environments

rnal effects may originate at different stages of the value net in
ed computer environments. Depending on the origin of the
ity, the individual decision-making calculus causing the externality
different. In any case decision makers focus on costs and benefits
to the individual agent and neglect costs or benefits of third parties.[6]

le 1 provides an overview of the sources and forms of externalities
vorked computer environment. The table captures the main
ders, but not necessarily all of them. Agents in the column are the

ame category. For example, the lax security policy of one ISP may xternalities for other ISPs.

irst source of possible externalities is software vendors. When g the level of investment in activities that reduce vulnerabilities, e vendors will only take their private costs and benefits into account er, 2000). Sales of software are dependent on the reputation of the this reputation effect is strong, the firm will also be concerned about rity situation of the software users. However, it is likely that such on effects are insufficient to fully internalise externalities. This is aggravated by the unique economics of information markets with gh fixed costs and low incremental costs, the existence of network which create first-mover advantages, and the prevalence of various of switching costs and lock-in. These characteristics provide an e for suppliers to rush new software to the market (Anderson, 2001; hostack, 2005). They may also lead to the dominance of one or a few ncreasing overall vulnerability due to a "monoculture" effect , 2005).

Table C.1. CERT.BR incident Reports

Software vendors	ISPs	Large firms	SMEs	Individual users	Criminals
Level of trust reputation	Risk of malevolent traffic	Level of software vulnerability	Level of software vulnerability	Level of software vulnerability	Hacking opportunities
Level of trust reputation	Volume of malevolent traffic	Risk of proliferating attack	Risk of proliferating attack	Risk of proliferating attack	Hacking opportunities
Level of trust reputation	Volume of malevolent traffic	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Hacking opportunities
Level of trust reputation	Volume of malevolent traffic	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Hacking opportunities
Level of trust reputation	Volume of malevolent traffic	Risk of hosting attack	Risk of hosting attack	Risk of hosting attack	Hacking opportunities
Level of trust reputation	Resource use reputation	Resource use Costs of crime	Resource use Costs of crime	Resource use Costs of crime	Hacking opportunities

, 2003; Camp and Wolfram, 2004; Schechter, 2004; Chen *et al*, owe and Gallaher, 2006). Profit-maximising firms, all other things qual, will attempt to invest in information security until the ited) incremental private benefits of enhanced security are equal to counted) costs of that investment. A firm will therefore not invest security risk is fully eliminated but only as long as the expected the threat are higher than the cost of increasing information security. at the firm imposes on third parties will not be considered in this (unless they indirectly affect a firm's decision making, for example, of reputation effects).

wise, benefits that a security investment bestows on third parties o not be reflected in this decision. Under conditions of imperfect tion and bounded rationality, firms may not be able to determine this optimum with precision but they will try to approximate it. In any ither the negative external effects of investments falling short of the ptimum nor the positive externalities of investments that go beyond imum are taken into consideration. Individual firm decisions may stematically deviate from a social optimum that takes these endencies into account.

vidual users are seen by many as one of the weakest links in the ain of networked computing (Camp, 2006). Larger business users onsider their decisions in an explicit cost-benefit framework. In , small business and individual users often do not apply such ental rationality (LaRose *et al*, 2005; Rifon *et al*, 2005). eless, when making decisions as to security levels, they consider n costs and benefits (but not those of other users). Individual users cularly susceptible to non-intrusive forms of malware, which do not significant resources on the user end (*e.g.* computing power, lth) but create significant damage to other machines. Consequently, of attack for all other users and the traffic volume on networks is d causing direct and indirect costs for third parties.

may inflict externalities on other agents in the value chain as well ach other. Some malware may increase traffic and hence ISP costs rementally. In this case, the ISP may have little incentive to incur al costs to engage in traffic monitoring and filtering. Even if users gnificant traffic increases, an ISP with a lot of spare capacity may anything but very incremental cost increases, again limiting the

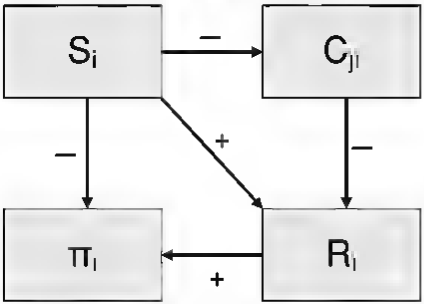
downtimes) and the cost of increased preventative security expenses
r stakeholders (including cost of software and security personnel).
costs include reduced trust within computer networks (for example,
maintain lists of trusted other systems) and of users in information
s, the ability of hackers to increase the effectiveness of attacks by
ng more machines, and the ability of hackers to hide their traces
and Wolfram 2004). They also include the potentially high costs
ed with the reduced willingness of consumers to engage in e-
ce

s in a dynamic framework

etworked computer environments with rapid technological change,
ities need to be understood in a dynamic framework. Most
ntly, learning and reputation effects need to be considered.
ion and learning may happen at different time scales and with
t intensity in the various components of the value net. They will also
ithin markets, for example enterprise market software as opposed to
arket software. In any case, they may counteract and reduce the
de of negative externalities and possibly enhance positive
ities. Moreover, the activities of firms to disclose vulnerabilities will
e the magnitude of externalities.

ure C.4 illustrates the reputation effect for the case of a software
plus and minus signs indicate whether the two variables move in the
the opposite direction). Other things being equal, lower expenses for
esting and refinement by firm i (S_i) will reduce sunk costs and hence
the profits (π_i) of the firm. However, costs may be externalised onto
rms, indexed j (C_{ji}). If these costs affect the reputation of firm i (R_i),
may be reduced, especially if the reputation effect works swiftly. In
e, at least part of the potential externality is internalised and the
n between private and social optimum is reduced. One form of
ening the reputation mechanism is trusted-party certification. As
n (2006) and Anderson (2001) point out, given present liability rules,
rms face an adverse selection incentive in that they do not face any
ences for issuing wrong certificates.

Figure C.4 Externalities with reputation



S_i security investment of firm i

C_{ji} cost for firm j cause by sub-optimal security investment by firm i

R_i reputation of firm i

π_i profits of firm i

dynamic perspective, the incentives to disclose vulnerabilities need onsidered (Cavusoglu *et al*, 2005). Disclosure exerts a positive ity (Gal-Or and Ghose, 2003, Gal-Or and Ghose, 2005) onto other ders. Under certain conditions, disclosure incentives may be ntly strong to shrink the conditions under which deviations between ate and social optimum occur to a minimum (Choi *et al*, 2005).

Notes

atements as to the effect of changes in individual parameters or factors e typically made under the *ceteris paribus* assumption that all other ngs remain equal. This is a widely used simplifying methodological ol to isolate changes in one or more variables in a highly complex terconnected system. Often, many factors will change simultaneously full grip on such changes will typically require some form of computer-sed modelling or simulation.

is possible that for some services and applications, 100% security levels e required (hence the benefits higher than the cost, even at a level of 0% security) and that the requisite cost will be incurred. It is unlikely, ough, that this will hold for all services and applications.

ore formally, the partial derivatives can be expressed as $\delta MBC/\delta S<0$, $MCC/\delta S>0$, $\delta MBS/\delta SV>0$, $\delta MCS/\delta SV>0$.

echanisms operating towards improving an objective are typically ferred to as "incentives" whereas those operating in the opposite rection are referred to as "disincentives."

is seems currently the case in many countries. See for example ɔindler, G. (2007), *Verantwortlichkeiten von IT-Herstellern, Nutzern d Intermediären. Studie im Auftrag des BSI durchgefuhrt von Prof. Dr. erald Spindler, Universitat Gottingen*, Bundesamt fur Sicherheit in der formationstechnik, *www.bsi.de/literat/studien/recht/Gutachten.pdf*.

a dynamic context, reputation effects may mitigate some of the ternalities, see the discussion below.

Glossary of Malware Terms

nentication factors: Used to obtain access; something the user knows
a password), something the user has (such as a credit card or
or something the user is (a photograph or thumbprint).

nentication/Authenticity: Being able to prove or verify a person's or
identity with a certain level of assurance. Authentication
isms are used to provide access control to information systems.

ilability: Ensuring that digital data within an information system and
em itself are available to authorised users.

kdoors[1]: A backdoor is malicious code that allows unauthorised
o a computer system or network by accepting remote commands
attacker elsewhere on the Internet.

jacking: Sending unsolicited messages to Bluetooth connected

snarfing enables unauthorised access to information from a wireless
hrough a Bluetooth connection.

programme: A type of 'backdoor' programme that allows attackers
otely control many compromised information systems (often
ds) simultaneously (or individually).

net(s): Group of malware infected computers that can be used to
y carry out attacks against other computer systems.

fidentiality: Being able to protect information and data from
rised access.

RTs: Computer emergency response teams.

RTs: Computer security incident response teams.

ital certificate A means of authenticating an identity for an entity oing business or other transactions on the web or on line. Digital tes exist as part of public key infrastructures (PKI)

main name The identifier or address of any entity on the Internet. Name System (DNS). The way Internet domain names are located nslated into an Internet Protocol, or IP, address. For example, the name www.oecd.org is a more user friendly and memorable ve to the IP address 193.51.65.71.

neynet Two or more honeypots on a network form a honeynet.

eypot is a trap set to detect, deflect or in some manner counteract at unauthorised use of information systems. Generally it consists of uter, data or a network site that appears to be part of a network but actually isolated, (un)protected and monitored, and which seems to information or a resource that would be of value to attackers.

grity A primary security goal of information systems which seeks to hat the system as a whole (people, data, software) have not been mised and can continue to be trusted. Internet Protocol. The native e of programmatic communication on the Internet.

stroke loggers[2] A hidden programme that records and "logs" each 's pressed on the compromised system's keyboard, as the legitimate he system is typing.

ware payload The primary function of a piece of malware.

-repudiation A security goal which seeks to prevent a person from they undertook an electronic transaction when they did.

rating system A computer program that manages the hardware and on a computer.

ket The minimum autonomously-routable quantum of data which ransmitted across a modern digital "packet switched" network.

ch/Workaround A small piece of software code designed to correct fy an existing bug or flaw in an operating system or application me. A work-around is a set of actions that network security rs can take to reduce their exposure to a known software

load The essential data that is being carried within a packet or other ssion unit. The payload does not include the "overhead" data l to get the packet to its destination.

tkit A set of programmes designed to conceal the compromise of a r at the most privileged "root" level, by modifying operating system nserting code into the memory of running processes.

al engineering Techniques designed to fool human beings into ng information or taking an action that leads to a subsequent breach nation systems security.

m Commonly understood to mean bulk, unsolicited, unwanted and lly harmful electronic messages.[3]

ofing is a technique designed to deceive an uninformed person about n of, typically, an e-mail or a website.

ware A form of malware that is capable of capturing a range of data er input (keyboards, mice) and output (screens) and other storage y, hard drive etc.) and sending this information to the attacker the user's permission or knowledge.

nsaction signing The process of calculating a keyed hash function to a unique string that can be used to verify both the authenticity and of an online transaction.

an horses A computer program that appears legitimate but actually den functionality used to circumvent security measures and carry out

s Directly analogous to its biological namesake, a virus is hidden t spreads by infecting another program and inserting a copy of itself program.

nerability A flaw or weakness in a system's design, implementation, ation and management of software that could be exploited.

m A type of malware that self replicates without the need for a host me or human interaction.

Bibliography

06), Zur Haftung von Phishing-Opfern *Arbeitsgruppe Identitatsschutz ternet e V, www a-i3 org/content/view/975/230/*

n, R (2001), "Why Information Security is Hard An Economic pective", Proceedings of the 17th Annual Computer Security ications Conference, New Orleans, Louisiana, IEEE Computer Society, *acsac org/2001/papers/110 pdf*

n, R (2002), "Unsettling Parallels between Security and the ronment", First Annual Workshop on Economics and Information rity, *www cl cam ac uk/~rja14/econws/37 txt*

n, R (2007), "Closing the Phishing Hole – Fraud, Risk and Nonbanks", *cl cam ac uk/~rja14/Papers/nonbanks pdf*

n, R and T Moore (2006), "The Economics of Information Security", *ce*, 314 610-613

n, R and T Moore (2007), "Information Security Economics – and nd", Computer Laboratory, University of Cambridge, *cl cam ac uk/~rja14/Papers/econ_crypto pdf*

n, R , *et al* (2008), "Security Economics and the Internal Market", pean Network and Information Security Agency, *enisa europa eu/doc/pdf/report_sec_econ_&_int_mark_20080131 pdf*

(2008), "Fraud abroad pushes up losses on UK cards following two- fall", press release, *www apacs org uk/2007Fraudfiguresrelease html*

Anti-Phishing Working Group) (2006a), *Phishing Activity Trends rt, www antiphishing org/reports/apwg_report_april_2007 pdf*, last ssed 14 December 2007

2006b), *Phishing Activity Trends Report, websense com/securitylabs/resource/PDF/apwg_report_december_200*

T and T I Tunca (2006), "Network Software Security and User
ntives, *Management Science*, 52(11) 1703–1720

T (2005), "Windows Rootkit, Prevention, Detection and Response",
auscert.org.au/, last accessed 11 December 2007

T (2006), "Haxdoor – An anatomy of an online ID theft Trojan",
auscert.org.au/render.html?cid=1920, last accessed 10 December,

an Government, Office of the Privacy Commissioner (2004),
munity Attitudes towards Privacy 2004
privacy.gov.au/publications/rcommunity/chap10.html, last accessed 11
mber 2007

an, E (2006), "Court likely to order ICANN to suspend Spamhaus' domain",
Technica, http://arstechnica.com/news.ars/post/20061009-7938.html

(2006) "Phishing: Kunden haften für Trojaner", Banktip.de,
banktip.de/News/20648/Phishing-Kunden-haften-fuer-Trojaner.html

S and M Gegick (2005), *Economy of Mechanism*, Build Security In,
://buildsecurityin.us-
gov/daisy/bsi/articles/knowledge/principles/348.html?branch=1&langu
1

M , *et al* (2008), "Financial Aspects of Network Security: Malware
Spam", International Telecommunication Union, July, *www.itu.int/ITU-*
b/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-
.pdf

ws (2004), "MyDoom virus biggest in months", BBC News website,
://news.bbc.co.uk/1/hi/technology/3432639.stm, last accessed 14
mber 2007

ws (2007a), "Google searches web's dark side", BBC News website,
://news.bbc.co.uk/2/hi/technology/6645895.stm

ws (2007b), "Burgers paid for by mobile phone", BBC News website,
://news.bbc.co.uk/2/hi/technology/6400217.stm, last accessed
cember, 2007

G S (1968), "Crime and Punishment: An Economic Approach",
Journal of Political Economy, 76(2) 169-217

(1999), "Economics and Crime in the States," *Economic Review* -

R and A Carter (2005), "The truth about credit-card fraud",
ness Week Online,
businessweek com/technology/content/jun2005/tc20050621_3238_tc02
n

n, D J (2007), "Some thoughts on security after ten years of qmail
1st Computer Security Architecture Workshop in conjunction with
ACM Conference on Computers and Communication Security, Fairfax,
ıma, *http://cr.yp.to/qmail/qmailsec-20071101.pdf*

R (2005), "Cyber-Insurance Revisited", Fourth Workshop on the
omics of Information Security, Harvard University,
//infosecon.net/workshop/pdf/15.pdf

, B (2007), "Spyware/Malware Impact on Consumers", APEC-OECD
ware Workshop, StopBadware Project, April,
oecd.org/dataoecd/33/55/38652920.pdf, last accessed 13 December

. J (2006), *Mental Models of Privacy and Security*,
//papers.ssrn.com/sol3/papers.cfm?abstract_id=922735

J and C Wolfram (2004), *Pricing Security Vulnerability as*
rnalities, http://ssrn.com/abstract=894966

ll, K , *et al* (2003), "The Economic Cost of Publicly Announced
mation Security Breaches Empirical Evidence from the Stock Market",
nal of Computer Security 11(3): 431-448,
//brief.weburb.dk/archive/00000130/01/2003-costs-security-on-
value-9972866.pdf

lu, H , B Mishra and S Raghunathan (2004), "The Effect of Internet
rity Breach Announcements on Market Value Capital Market
tions for Breached Firms and Internet Security Developers",
national Journal of Electronic Commerce, 9(1): 69,
gvsu.edu/business/tjec/v9n1/p069.html

lu, H , H Cavusoglu and S Raghunathan (2005), *Emerging issues in*
onsible vulnerability disclosure, Fourth Workshop on the Economics of
mation Security, Harvard University,
//infosecon.net/workshop/pdf/cavusoglu.pdf

United States Computer Emergency Response Team),
ral Incident Reporting Guidelines,
us-cert.gov/federal/reportingRequirements.html

oordination Center (2007), The Use of Malware Analysis in Support of Enforcement,
securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement, last accessed 11 mber 2007

, S. (2005), "Combating Cybercrime: A Public-Private Strategy in the al Environment", Microsoft Corporation,
nwacc org/programs/conf05/UNCrimeCongressPaper doc, last ssed 11 December 2007

-Y , G. Kataria and R. Krishnan (2005) "Software Diversity for mation Security", Fourth Workshop on the Economics of Information rity, Harvard University, http //infosecon net/workshop/pdf/47 pdf

P , C. Fershtman and N. Gandal (2005), "Internet Security, erability Disclosure, and Software Provision", Fourth Workshop on the omics of Information Security, Harvard University, //infosecon net/workshop/pdf/9 pdf

R. (2007), "Phishing and the gaming of 'clue'", Light Blue hpaper, www lightbluetouchpaper org/2007/08/16/phishing-and-the-ng-of-clue/.

er Economics (2007), 2007 Malware Report: The Economic Impact of es, Spyware, Adware, Botnets and other malicious code,
computereconomics.com/page.cfm?name=Malware%20Report

sional Budget Office Cost Estimate (2007), "H.R. 1525 Internet vare (I-SPY) Prevention Act of 2007", as ordered reported by the House mittee on the Judiciary, 7 May,
cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf

er Reports WebWatch (2005), "Leap of Faith: Using the Internet ite the Dangers", results of a National Survey of Internet Users for umer Reports WebWatch, www consumerwebwatch.org/dynamic/web-bility-reports-princeton.cfm ;

ers Union (2007), "State of the 'Net' Survey '07", *Consumer Reports*, (9), 28-34.

entenbond (2006), "PC beveiliging & veilig Internet: Een enquête onder uitergebruikers", *Consumentengids*, 2006(11)

of Europe (2001), *Convention on Cybercrime*, Budapest, 23 November,

pane & MessageLabs (2006), *2005 Attack Trends & Analysis*,
counterpane.com/dl/attack-trends-2005-messagelabs.pdf

mputer Security Institute) (2007), *CSI Survey 2007- The 12th Annual*
puter Crime and Security Survey,
gocsi.com/forms/csi_survey.jhtml

Computer Crime and Security Survey (2006),
gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=4SCJQ3Y0PCPT
NDLPCKHSCJUNN2JVN

D. (2006), "Malware – future trends",
linuxsecurity.com/docs/malware-trends.pdf, last accessed 7 December

K. (2007), "Online security begins at home", *Australian IT News*,
//australianit.news.com.au/articles/0,7204,21675098%5E24169%5E%5
%5E,00.html, last accessed 11 December 2007

, D. (2000), "Statement by Dorothy E. Denning", Georgetown
ersity, *http://fip.fas.org/irp/congress/2000_hr/00-05-23denning.htm*

d, A. (2006), *Le « phishing » en France, peu de victimes mais une*
ace grandissante, 01net,
01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-
de-victimes-mais-une-menace-grandissante/, last accessed 11 December

, Rachna, *et al.* (2007), "The Emperor's New Security Indicators, An
ation of website authentication and the effect of role playing on
lity", *http://usablesecurity.org/emperor*

(2007), "Dot Tk Free Domain Names – A New Approach To Make A
le Top Level Country Domain Free Of Illicit Content",
dot.tk/en/press_jul16_07.pdf

2007), "Introduction of malware Issues", presentation by CNCERT/CC
APEC-OECD Malware Workshop,
oecd.org/dataoecd/33/59/38653107.pdf, last accessed 10 December,

S., E. Andrijcic and M. E. Johnson (2006), "Costs to the U.E. Economy
formation Infrastructure Failure from Field Studies and Economic
", Fifth Workshop on the Economics of Information Security 2006,
//weis2006.econinfosec.org/docs/4.pdf

nomist (2007), "A cyber riot", 10 May,
economist.com/world/europe/displaystory.cfm?story_id=9163598,
ssed 4 December, 2007.

, L , (2004), "Reconstruction Consumer Privacy Protection Online",
national Review of Law – Computers & Technology, Vol. 18, No. 3, p

I. J. van and J. M. Bauer (2008), "Economics of Malware: Security
sions, Incentives and Externalities", *OECD Science, Technology and*
stry Working Papers, 2008/1, OECD Publishing,
0.1787/241440230621

I. (1996), "Crime, Punishment, and the Market for Offenses", *The*
nal of Economic Perspectives, 10(1): 43-67,
//links.jstor.org/sici?sici=0895-
%28199624%2910%3A1%3C43%3ACPATMF%3E2.0.CO%3B2-U

European Network and Information Security Agency) (2006), *Provider*
rity Measures Part 1. Security and Anti-Spam Measures of Electronic
munication Service Providers - Survey,
enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf

Young (2007), *Global Information Security Survey 2006*,
ey.nl/download/publicatie/2006_GISS_EYG_AU0022.pdf

n Union (1995), "Directive 95/46/EC of the European Parliament and of
ouncil of 24 October 1995 on the protection of individuals with regard
e processing of personal data and on the free movement of such data",
tal Journal of the European Communities, L 281/31,
//ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-
art1_en.pdf, accessed 11 December 2007

n Union (2002), "Directive 2002/58/EC of the European Parliament and
ouncil of 12 July 2002 Concerning The Processing Of Personal Data
The Protection Of Privacy In The Electronic Communications Sector",
nal Journal of the European Communities, L 201/37, *http://eur-*
uropa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.
accessed 11 December 2007.

n Union (2005), "Council Framework Decision 2005/222/JHA of 24
uary 2005 on attacks against information systems", *Official Journal of*
uropean Communities, L 69/67 *http://eur-*
uropa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.

2007), *Consumer Reports: Putting Consumers Back in Control*, Federal
e Commission,
ftc.gov/bcp/workshops/spamsummit/presentations/Consumers.pdf

, J , *et al* (2007), "An Inquiry into the Nature and Causes of the Wealth
ternet Miscreants", CCS'07, *www.ictr.org/vern/papers/miscreant-
th.ccs07.pdf*

n, L S (2002), *The Microeconomics of Public Policy Analysis*,
eton University Press, Princeton

(2007), "IT Security Threat Summary for H1 2007", F-Security Data
rity Wrapup 1/2007, *www.f-secure.com/2007/1/*

E and A Ghose (2003), "The Economic Consequences of Sharing
rity Information", 2nd Annual Workshop on Economics and
mation Security,
cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf

E and A Ghose (2005), "The Economic Incentives for Sharing
rity Information", *Information Systems Research*, 16(2) 186-208.
andrew.cmu.edu/user/aghose/Infosec.pdf

(2005), "Gartner Survey Shows Frequent Data Security Lapses and
ased Cyber Attacks Damage Consumer Trust in Online Commerce",
release, *www.gartner.com/press_releases/asset_129754_11.html*

S (2007), "T J Maxx Security Breach Costs Soar To 10 Times Earlier
nate", *Information Week*,
*//www.informationweek.com/shared/printableArticle.jhtml?articleID=2
00259*

Online (2006), *The Get Safe Online Report*, October,
getsafeonline.org/media/GSO_Cyber_Report_2006.pdf

Inc (2007), "The Ghost In The Browser Analysis of Web-based
vare",
usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf,
ssed 12 December 2007

L A and M P Loeb (2002), "The Economics of Information Security
stment", *ACM Transactions on Information and System Security*, Vol 5,
4, pp 438-457, *http://portal.acm.org/citation.cfm?id=581274*

nl (2006), *Annual Review*, *www.govcert.nl/render.html?it=147*, last
ssed 13 December 2007

T (2007), "Kapersky seeks help from international police to fight rcrime", *Network World, www networkworld com/news/2007/013107-rsky-cybercrime html*, accessed 14 December 2007

, J (2007), "IP-Blacklisting zur Spam-Abwehr kann rechtswidrig sein", *e Online, www heise de/newsticker/meldung/97568*

K J (2007a), "Battling Bots, Doing No Harm", *Dark Reading, darkreading com/document asp?doc_id=118739*

K J (2007b), "Untying the Bot Knot", *Dark Reading, darkreading com/document asp?doc_id=114081&WT svl=news1_6*

t Project and Research Alliance (2007), *Know your enemy Fast-Flux ce Networks, www honeynet org/papers/fff/*, accessed 13 December,

f Lords (2007a), *Science and Technology Committee, 5th Report of on 2006–07, Personal Internet Security, Volume I Report*, Authority of louse of Lords, *www publications parliament uk/pa/ld/ldsctech htm*

f Lords (2007b), *Science and Technology Committee, 5th Report of on 2006–07, Personal Internet Security, Volume II Evidence*, ority of the House of Lords, *publications parliament uk/pa/ld/ldsctech htm*

en, M (2006), "Malware goes mobile", *Scientific American*, pp 70-77, *cs virginia edu/~robins/Malware_Goes_Mobile pdf*, accessed 13 mber 2007

esearch, Inc (2006), "The Trusted Computing Group Mobile ification Securing Mobile Devices on Converged Networks", White r, September, *trustedcomputinggroup org/groups/mobile/Final_iGR_mobile_security te_paper_sept_2006 pdf*, accessed 7 December 2007

ernational Telecommunications Union) (2007), "Executive Summary", *d Information Society Report 2007 Beyond WSIS, itu int/osg/spu/publications/worldinformationsociety/2007/WISR07-mary pdf*

Strategy & Research (2007), *2007 Identity Fraud Survey Report – umer Version How Consumers Can Protect Themselves, acxiom com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Repo 7200734724 pdf*, accessed 14 December 2007

ky Labs (2006), *Malware Evolution 2006. Executive Summary*, *kaspersky com/malware_evolution_2006_summary*

(2006), "The New Face of Phishing", Washington Post Security Fix og, *//blog washingtonpost com/securityfix/2006/02/the_new_face_of_phishi html*

(2007), "Study $3 2 Billion Lost to Phishing in 2007", Washington Security Fix weblog, *//blog washingtonpost com/securityfix/2007/12/study_32_billion_lost_to sh_1 html*

(2008), "Banks Losses from Computer Intrusions Up in 2007", ington Post Security Fix weblog, *//blog washingtonpost com/securityfix/2008/02/banks_losses_from_com _int html*

her, H and G Heal (2003), "Interdependent security", *Journal of Risk Uncertainty*, 26(2) 231

, H , S Crane and A Phippen (2006), "Trustguide Final Report", BT p Chief Technology Office, Research & Venturing / HP Labs / ersity of Plymouth, Network Research Group, *trustguide org uk/Trustguide%20-%20Final%20Report.pdf*

R , N Rifon, S Liu and D Lee (2005), "Understanding Online Safety vior. A Multivariate Model", International Communication ciation, New York, *www msu.edu/~isafety/papers/ICApanelmult21 htm*

R (2006), "Attackers pass on OS, aim for drivers and apps", Security s website, *www securityfocus com/news/11404*

R (2007), "Estonia gets respite from web attacks", Security Focus ite, *www securityfocus com/brief/504*

V (2007), "Panel Discussion Gaps and Challenges", presentation at the D-APEC Tel Malware Workshop by the Director of the Information Communication Security Technology Center, Chinese Taipei, *oecd org/dataoecd/34/19/38653499 pdf*, accessed 10 December 2007

Inc (2006), "Virtual Criminology Report 2007 Organized Crime and nternet", *McAfee Avert® Labs Technical White Papers*, December, *mcafee com/us/threat_center/white_paper html*

Inc (2007), "Identity Theft", *McAfee Avert® Labs Technical White*

y, C. (2007), "Study: Identity theft keeps climbing", *Cnet News*, *//news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-765.html*.

ara, P. (2007), "Survey: Identity theft on the decline", *Network World*, *networkworld.com/community/?q=node/11009*, accessed 11 December

l, A. (1920), *Principles of Economics: An Introductory Volume*, millan, London

sky, Y. (2007), "The Virtual Conflict – Who Will Triumph?", *The alist, www.viruslist.com/en/analysis?pubid=204791915*

K. Kent and J. Nusbaum (2005), *Guide to Malware Incident ention and Handling*, National Institute of Standards and Technology, *//csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*

ng Anti-Abuse Working Group (2007), "Email Metrics Program: The ork Operators' Perspective, Report #5 - First Quarter 2007, June 2007", *maawg.org/about/MAAWG20071Q_Metrics_Report.pdf*, accessed 10 mber 2007

UK National Infrastructure Security Information Centre) (2005), geted TrojanEmail Attacks", *NISCC Briefing*, 08/2005, *cpni.gov.uk/docs/ttea.pdf*, accessed 7 December 2007.

Labs (2006), *MessageLabs Intelligence: 2006 Annual Security Report - ar of Spamming Dangerously: The Personal Approach to Attacking*, *messagelabs.com/mltreport/2006_annual_security_report_5.pdf*, ssed 10 December 2007.

labs (2007), *MessageLabs Intelligence: 2007 Annual Security Report - ar of storms, spam and socializing*, *messagelabs.com/resources/mltreports*, accessed 10 December 2007.

r, E. and D. Pappalardo (2005), "Extortion via DDoS: on the rise: finals are using the attacks to extort money from victimized companies", *puterworld*, *computerworld.com/networkingtopics/networking/story/0,10801,10176.html*, accessed 7 December 2007.

ft (2005), *The Trustworthy Computing Security Development Lifecycle*, *//msdn2.microsoft.com/en-us/library/ms995349.aspx*

ft (2006a), *Security Intelligence Report (January – June 2006)*

ft (2006b), *Security Intelligence Report (July - December 2006)*, *microsoft com/downloads/details aspx?familyid=af816e28-533f-4970-e35dc3f26cfe&displaylang=en*, accessed 3 December 2007

ft (2007), "Storm Drain", Anti-Malware Engineering Team Weblog, *//blogs technet com/antimalware/archive/2007/09/20/storm-drain aspx*

Toolbar Community (2007), "Phishing By The Numbers 609,000 ked Sites in 2006", Netcraft website, *//news netcraft com/archives/2007/01/15/phishing_by_the_numbers_60_blocked_sites_in_2006 html*, accessed 11 December 2007

lational Institute of Standards and Technology) (2005), *Guide to ware and Incident Handling, Recommendations of the National Institute andards and Technology*, Special Publication 800-83, November, *//csrc nist gov/publications/nistpubs/800-83/SP800 83 pdf*

008), *Computer Security Handling Guide Recommendations of the onal Institute of Standards and Technology*, Special Publication 800-61 sion 1, March *http //csrc nist gov/publications/nistpubs/800-61-/SP800-61rev1 pdf*

y, E (1987), *Der offentliche Sektor Einfuhrung in die nzwissenschaft*, Springer, Berlin

S (2007), "Addressing the Malware Problem", presentation given at the C-OECD Malware Workshop, *//www oecd org/dataoecd/33/57/38653049 pdf*

2002a), *OECD Guidelines for the Security of Information Systems and orks Towards a Culture of Security*, *oecd org/dataoecd/16/22/15582260 pdf*

2002b) "OECD Guidelines for the Security of Information Systems and orks Towards a Culture of Security – Questions and Answers", *oecd org/dataoecd/27/6/2494779 pdf*

2005a), "The Promotion of a Culture of Security for Information ms and Networks in OECD Countries", unclassified document of the king Party on Information Security and Privacy, l/ICCP/REG(2005)1/FINAL, 16 December, *oecd org/dataoecd/16/27/35884541 pdf*

2005b), *Science, Technology, and Industry Scoreboard*, 2005 edition, D Publishing, Paris

2007a), *OECD Communications Outlook 2007*, Information and
munications Technologies, OECD Publishing, Paris

2007b), "APEC-OECD Malware Workshop. Summary Record",
assified document of the Working Party on Information Security and
icy, DSTI/ICCP/REG(2007)15, 15 June,
oecd.org/dataoecd/37/60/38738890.pdf

2007c), "The Development of Policies for the protection of Critical
rmation (CII). A comparative analysis in four OECD countries: Canada,
a, the United Kingdom and the United States", unclassified document
e Working Party on Information Security and Privacy,
I/ICCP/REG(2006)15/FINAL, 6 February,
*olis oecd org/olis/2006doc nsf/ENGREFCORPLOOK/NT00007766/$F
/JT03221273.PDF*

2008a), "The Development of Policies for the protection of Critical
rmation (CII). A comparative analysis in three OECD countries:
ralia, Japan, and the Netherlands", unclassified document of the
king Party on Information Security and Privacy,
I/ICCP/REG(2007)16/FINAL, 9 January,
*olis.oecd.org/olis/2007doc nsf/ENGREFCORPLOOK/NT00005A5E/$F
/JT03238526.PDF*

2008b), "Scoping Paper on Online Identity Theft", unclassified
ment, DSTI/CP(2007)3/FINAL, 15 May,
*olis oecd org/olis/2007doc nsf/ENGREFCORPLOOK/NT00005CAE/$
/JT03240674.PDF*

2008c), "The Development of Policies for the Protection of Critical
rmation Infrastructures (CII). A Comparative Analysis in Seven OECD
ntries: Australia, Canada, Korea, Japan, The Netherlands, The United
dom and the United States", unclassified document of the Working
y on Information Security and Privacy,
I/ICCP/REG(2007)20/FINAL, 8 April,
*//www olis oecd org/olis/2007doc nsf/ENGREFCORPLOOK/NT00005A
FILE/JT03243745.PDF*

007), *Spamhaus antwortet auf nic at*, futurezone,
//futurezone.orf.at/it/stories/201738/, accessed 25 November 2007

rom (2007), "Phishing attack evades ABN Amro's two-factor
ntication", OUT-LAW News, 18 April, *www out-law com/page-7967*,
ssed 11 December 2007

ler, J. C., J. B. Earp and D. L. Baumer (2006), "An experimental
omics approach toward quantifying online privacy choices",
mation Systems Frontiers, 8(5) 363-374.

Kevin (2003), *Slammer worm crashed Ohio nuke plant network*,
rity Focus, *www securityfocus com/news/6767*, accessed 11 December

(2007), "Phishing attack evades bank's two-factor authentication",
theregister.co uk/2007/04/19/phishing_evades_two-
r_authentication/

, E. (2004), "Is finding security holes a good idea?", Workshop on
omics and Information Security 2004, *www rtfm com/bugrate pdf*

., E. T. Quilliam and R. LaRose (2005), "Consumer Perceptions of
ie Safety", paper presented at the International Communication
ciation, Communication and Technology Division, New York, 27 May,
msu edu/~isafety/papers/ICApanelfg htm

R. and M. P. Gallaher (2006), "Private Sector Cyber Security
stment: An Empirical Analysis", Fifth Workshop on the Economics of
mation Security, Cambridge, March,
weis2006 econinfosec org/docs/18 pdf

urity (2006), "Internet Confidence Index Shows that – for Businesses
Consumers – Transactions are Outpacing Trust",
rsa com/press_release aspx?id=6502, accessed 14 December 2007

r, S. E. (2004), *Computer Security Strength & Risk: A Quantitative*
oach, thesis presented to the Division of Engineering and Applied
nces, Harvard University, May,
eecs harvard edu/~stuart/papers/thesis pdf

, B. (2000), *Secrets and Lies: Digital Security in a Networked World*,
Wiley, New York.

, B. (2005), "A Real Remedy for Phishers", *Wired News*,
wired com/news/politics/0,1283,69076,00 html

, B. (2007), "Information Security and Externalities", NSF/OECD
kshop on Social & Economic Factors Shaping The Future of the
net, Washington, DC, *www oecd org/dataoecd/60/8/37985707 pdf*

T. (2007), "Lose an unencrypted laptop and 'face criminal action'",
nterworld UK, 15 November.

(2007a), "Is Identity Theft Decreasing?", The Checkout Washington Blog, 6 February, *//blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decre* *html*

(2007b), "Looking for a Job? Phishers Are Looking for You ", The kout Washington Post Blog, 12 February, *//blog.washingtonpost.com/thecheckout/2007/02/looking_for_a_job_phi* *_are.html*

., A (2005), "Avoiding Liability An Alternative Route to More Secure ucts", Fourth Workshop on the Economics of Information Security, ard University, *infosecon.net/workshop/pdf/44.pdf*

W (2007), "Time to Deploy improvement of 25 %", Mozilla Security , *http //blog.mozilla.com/security/2007/06/18/time-to-deploy-* *ovement-of-25-percent/*

, D A (2007), "Spamhaus.org setzt Osterreichs Domainverwaltung Druck", Heise online, *www.heise.de/newsticker/meldung/91417*, last ssed 25 November 2007

2006a), "The Growing Scale of the Threat Problem", *sophos.com/sophos/docs/eng/papers/Growing-threat-wpus.pdf*, ssed 7 December, 2007

2006b), "Devious Arhiveus ransomware kidnaps data from victims puters", *sophos.com/pressoffice/news/articles/2006/06/arhiveus.html*, accessed mber 7, 2007

2006c), "Married couple formally charged over spyware Trojan horse", *sophos.com/pressoffice/news/articles/2006/03/tsraeltesp2.html*, ssed 13 December 2007

2007a), "Security Threat Report", Sophos Security white paper, *sophos.com/security/whitepapers/*, last accessed 12 December 2007

2007b), "Security Threat Report Update July 2007", Sophos Security paper, *www.sophos.com/security/whitepapers/*, accessed 12 December

(2007), "Web issues over banking code", *The New Zealand Herald*, *nzherald.co.nz/topic/story.cfm?c_id=126&objectid=10458545*

is (2007), "Report on the criminal Rock Phish domains registered at

OECD PUBLISHING 2 rue André Pascal 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(93 2009 01 1 P) ISBN 978 92-64 05650 3 – No 56607 2009

Computer Viruses and Other Malicious Software

A THREAT TO THE INTERNET ECONOMY

The Internet has become a powerful tool for enhancing innovation and productivity. Nevertheless, the increasing dependence on the Internet and other communication networks means the Internet has also become a popular and efficient way to spread computer viruses and other types of malicious software (malware).

Malware attacks are increasing in both frequency and sophistication, thus posing a serious threat to the Internet economy and to national security. Concurrently, efforts to fight malware are not up to the task of addressing this growing global threat: malware response and mitigation efforts are essentially fragmented, local and mainly reactive.

A wide range of communities and actors – from policy makers to Internet Service Providers to end users – all play a role in combating malware. But there is still limited knowledge, understanding, organisation and delineation of the roles and responsibilities of each of these actors. Improvements can be made in many areas, and international co-operation would benefit greatly in areas such as: proactive prevention (education, guidelines and standards); research and development; improved legal frameworks; stronger law enforcement; improved tech industry practices; and better alignment of economic incentives with societal benefits.

This book is a first step toward addressing the threat of malware in a comprehensive, global manner. It has three major aims: 1) to inform policy makers about malware – its growth, evolution and countermeasures to combat it; 2) to present new research into the economic incentives driving cyber security decisions; and 3) to make specific suggestions on how the international community can better work together to address the problem.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-05650-3
83 2009 01 1 P